Dell™ PowerConnect™ M6220/M6348/M8024

User's Guide

Model M6220/M6348/M8024

www.dell.com | support.dell.com

Downloaded from www.Manualslib.com manuals search engine

Notes, Notices, and Cautions

A NOTE indicates important information that helps you make better use of your switch.

A NOTICE indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

A CAUTION indicates a potential for property damage, personal injury, or death.

Information in this document is subject to change without notice.
© 2009 Dell Inc. All rights reserved.

Reproduction in any manner whatsoever without the written permission of Dell Inc. is strictly forbidden.

Trademarks used in this text: *Dell*, the *DELL* logo, *PowerEdge, PowerConnect,* and *OpenManage* are trademarks of Dell Inc.; *Microsoft* and *Windows* are registered trademarks of Microsoft Corporation.

Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Dell Inc. disclaims any proprietary interest in trademarks and trade names other than its own.

Model M6220/M6348/M8024

June 2009 **Rev. A01**

Downloaded from www.Manualslib.com manuals search engine

Contents

1 Introduction

Switching Features **18**

Virtual Local Area Network Supported Features 21

Link Aggregation Features 24

MAC Address Supported Features 26

IPv4 Routing Features 27

IPv6 Routing Features 28

IPv6 . . . . . **28**

Quality of Service Features **29**

Multicast Features **30**

IPv4 Multicast Features 30

IPv6 Multicast Features 31

Security Features 31

CLI Documentation **32**

2 Using Dell™ OpenManage™ Switch Administrator

Verifying the Out-of-Band (OOB) IP Address 34

Setting a Static IP Address 34

Understanding the Interface **35**

Information Buttons 40

Device Management Buttons 40

Defining Fields **41**

Accessing the Switch Through the CLI **41**

Telnet Connection 42

Using the CLI **42**

Command Mode Overview 42

User EXEC Mode 43

Privileged EXEC Mode 43

Global Configuration Mode 44

Interface Configuration Mode 44

Downloaded from www.Manualslib.com manuals search engine

3 Cable and Port Information

Overview **45**
Connecting the Switch to a Terminal 48

Power Connection **48**

4 Hardware Description

Overview **49**
Physical Dimensions 53
Power Supplies 53
Ventilation System 53
Stacking 54
PowerConnect LED Definitions 56

5 Configuring Dell™ PowerConnect™

Overview **63**

Starting the CLI **64**

General Configuration Information **66**
Terminal Connection Configuration 66
Other Configuration Requirements 66

Booting the Switch **67**

Configuration Overview **73**
Easy Setup Wizard 73

Advanced Configuration **78**
CLI Basics 78
M6220, M6348, and M8024CLI Reference Guide 80
Security Management and Password Configuration 83
Software Download Through TFTP Server 85
Update Bootcode 87

Boot Menu Functions **87**
Start Operational Code 88
Change the Baud Rate 88
Retrieve Event Log using XMODEM 89
Load New Operational Code Using XMODEM 89

Downloaded from www.Manualslib.com manuals search engine

Display Operational Code Vital Product Data 90
Update Boot Code. 91
Reset the System 92
Restore Configuration to Factory Defaults 92
Password Recovery Procedure 93

Sample Configuration Process 93
Initial Connection 94
Device Default Settings. 99
Enabling Remote Management. 99
Configuring Secure Management Access (HTTPS) 102

6 Configuring System Information

Overview 103
Asset 104
System Health. 106
Versions. 107
System Resources 108
Time Zone Configuration 109
Summer Time Configuration 110
Clock Detail 112
Reset 113
SNTP Global Settings. 115
SNTP Authentication 116
SNTP Server 119

Managing Logs. 122
Global Settings 122
RAM Log Table 125
Log File 126
Remote Log Server Settings 127

Setting the Operational Mode 130
Operational Mode Configuration 130

Defining IP Addressing 132
Domain Name Server (DNS) 134
Default Domain Name 135
Host Name Mapping 137
Dynamic Host Name Mapping 139

Downloaded from www.Manualslib.com manuals search engine

ARP Table 140
IPv6 Management Features 141

Running Cable Diagnostics 143
Integrated Cable Test for Copper Cables 143
Optical Transceiver Diagnostics 145

Managing Device Security 147
Access Profile 148
Authentication Profiles 153
Select Authentication 157
Password Management 161
Local User Database 162
Line Passwords 165
Enable Password 167
TACACS+ Settings 168
RADIUS Global Configuration 171
RADIUS Server Configuration 173
RADIUS Accounting Server Configuration 176
RADIUS Accounting Server Statistics 179
RADIUS Server Statistics 180
Authorization Network RADIUS 181
Telnet Server 183
Denial of Service 184

Captive Portal 186
CP Global Configuration 187
CP Configuration 188
CP Web Customization 191
Local User 194
User Group 196
Interface Association 198
CP Status 200
CP Activation and Activity Status 201
Interface Activation Status 202
Interface Capability Status 203
Client Summary 204
Client Detail 205
CP Interface Client Status 205
CP Client Status 206

Downloaded from www.Manualslib.com manuals search engine

Defining SNMP Parameters **207**
SNMP v1 and v2 207
SNMP v3 207
SNMP Global Parameters 208
SNMP View Settings 209
Access Control Group 212
SNMPv3 User Security Model (USM) 215
Communities 219
Notification Filter 222
Notification Recipients 225

File Management **229**
File System 229
Active Images 230
File Download 230
File Upload 233
Copy Files 234

Defining Advanced Settings **236**
Auto Configuration 236

Defining Stacking **238**
Stacking Standby 238
Unit Configuration 238
Stack Summary 240
Supported Switches 241
Stack Port Summary 243
Stack Port Counters 244
Stack Port Diagnostics 245

sFlow **245**
sFlow Agent Summary 246
sFlow Receiver Configuration 247
sFlow Sampler Configuration 249
sFlow Poll Configuration 251

Industry Standard Discovery Protocol **253**
ISDP Global Configuration 253
Cache Table 255
Interface Configuration 256
ISDP Statistics 257

Downloaded from www.Manualslib.com manuals search engine

7 Configuring Switching Information

Overview **259**

Dot1x Authentication 260

Authenticated Users 265

Port Security 266

IP ACL Configuration 267

IP ACL Rule Configuration 270

MAC ACL Configuration. 273

MAC ACL Rule Configuration 275

IPv6 Access Control Lists. 277

IPv6 ACL Rule Configuration 279

ACL Bind Configuration 283

Configuring Ports. **285**

Global Parameters 285

Port Configuration. 286

Protected Port Configuration 290

LAG Configuration. 292

Storm Control 294

Configuring Traffic Mirroring **296**

Port Mirroring 296

Flow Based Mirroring. 299

Configuring Address Tables **300**

Static Address Table 300

Dynamic Address Table. 303

Configuring GARP **305**

GARP Timers 305

Configuring the Spanning Tree Protocol **308**

STP Global Settings. 308

STP Port Settings 310

STP LAG Settings 313

Rapid Spanning Tree 316

MSTP Settings 318

MSTP Interface Settings 320

Configuring VLANs. **322**

VLAN Membership 323

Double VLAN 326

Downloaded from www.Manualslib.com manuals search engine

VLAN Port Settings 330
VLAN LAG Settings 333
Bind MAC to VLAN 335
Bind IP Subnet to VLAN. 337
Protocol Group 339
GVRP Parameters. 342

Configuring Voice VLAN **345**

Aggregating Ports **347**
LACP Parameters 347
LAG Membership 349
LAG Hash Configuration 351
LAG Hash Summary. 352

Managing Multicast Support **353**
Multicast Global Parameters 354
Bridge Multicast Group. 355
Bridge Multicast Forward. 359

IGMP Snooping. **360**
General IGMP Snooping 361
Global Querier Configuration 363
VLAN Querier 365
VLAN Querier Status 367
MFDB IGMP Snooping Table 368

MRouter Status. **369**

MLD Snooping **370**
MLD Snooping General 370
MLD Snooping Global Querier Configuration. 372
MLD Snooping VLAN Querier. 373
MLD Snooping VLAN Querier Status 375
MFDB MLD Snooping Table 376

Configuring the Link Layer Discovery Protocol (LLDP) **377**
LLDP Configuration 377
LLDP Statistics 380
LLDP Connections. 382

Creating Link Dependencies. **384**
Link Dependency Summary. 384

Downloaded from www.Manualslib.com manuals search engine

Dynamic ARP Inspection **387**
DAI Global Configuration 387
DAI Interface Configuration 388
DAI VLAN Configuration 390
DAI ACL Configuration 391
DAI ACL Rule Configuration. 392
DAI Statistics 394

DHCP Snooping **395**
DHCP Snooping Configuration 396
DHCP Snooping Interface Configuration 397
DHCP Snooping VLAN Configuration 399
DHCP Snooping Persistent Configuration 400
DHCP Snooping Static Bindings Configuration. 401
DHCP Snooping Dynamic Bindings Summary 403
DHCP Snooping Statistics 405
IP Source Guard 406

DHCP Relay. **408**
DHCP Relay Global Configuration 409
DHCP Relay Interface Configuration 410
DHCP Relay Interface Statistics 411
DHCP Relay VLAN Configuration 413

Using the Port Aggregator Feature **414**
Port Configuration Summary 415
Group Configuration Summary 417
Group VLAN MAC Summary 420

8 Viewing Statistics and Remote Monitoring

Overview **421**

Table Views **422**
Interface Statistics 422
Etherlike Statistics 424
GVRP Statistics 425
EAP Statistics 427
Utilization Summary. 429
Counter Summary. 430

Downloaded from www.Manualslib.com manuals search engine

RMON 431
RMON Statistics 432
RMON History Control Statistics 434
RMON History Table 436
RMON Event Control 438
RMON Event Log 441
RMON Alarms 442

Charts 446
Ports Statistics 446
LAG Statistics 448

9 Configuring Routing

Overview 451
ARP Create 453
ARP Table Configuration 454

IP 456
IP Configuration 456
IP Statistics 458
IP Interface Configuration 461

OSPF 463
OSPF Configuration 464
Area Configuration 467
Stub Area Summary 470
Area Range Configuration 471
Interface Statistics 473
Interface Configuration 475
Neighbor Table 480
Neighbor Configuration 481
Link State Database 484
Virtual Link Configuration 485
Virtual Link Summary 491
Route Redistribution Configuration 493
Route Redistribution Summary 496

BOOTP/DHCP Relay Agent 497
BOOTP/DHCP Relay Agent Configuration 498
BOOTP/DHCP Relay Agent Status 499

Downloaded from www.Manualslib.com manuals search engine

IP Helper **500**
IP Helper Global Configuration 501
IP Helper Interface Configuration 504
IP Helper Statistics 506

RIP **507**
RIP Configuration 508
RIP Interface Summary 510
RIP Interface Configuration. 512
RIP Route Redistribution Configuration. 514
RIP Route Redistribution Summary 517

Router Discovery **518**
Router Discovery Configuration 518
Router Discovery Status 520

Router. **521**
Route Table 522
Best Routes Table. 523
Route Entry Configuration. 525
Configured Routes 528
Route Preferences Configuration. 529

VLAN Routing. **531**
VLAN Routing Configuration 532
VLAN Routing Summary 533

VRRP **534**
VRRP Router Configuration 535
VRRP Virtual Router Status 540
VRRP Virtual Router Statistics 542

Tunnels **544**
Tunnels Configuration. 545
Tunnels Summary 548

Loopbacks **549**
Loopbacks Configuration 550
Loopbacks Summary 556

Downloaded from www.Manualslib.com manuals search engine

10 Configuring IPv6

Overview **557**

Global Configuration **558**

Interface Configuration **559**

Interface Summary **562**

IPv6 Statistics **563**

IPv6 Neighbor Table **568**

DHCPv6 . . . . . **569**

DHCPv6 Global Configuration 570
DHCPv6 Pool Configuration 572
Prefix Delegation Configuration 575
DHCPv6 Pool Summary 577
DHCPv6 Interface Configuration 578
DHCPv6 Server Bindings Summary 581
DHCPv6 Statistics 582

OSPFv3 . . . . . **584**

OSPFv3 Configuration 585
OSPFv3 Area Configuration 588
OSPFv3 Stub Area Summary 592
OSPFv3 Area Range Configuration 593
OSPFv3 Interface Configuration 595
OSPFv3 Interface Statistics 598
OSPFv3 Neighbors 600
OSPFv3 Neighbor Table 603
OSPFv3 Link State Database 605
OSPFv3 Virtual Link Configuration 607
OSPFv3 Virtual Link Summary 610
OSPFv3 Route Redistribution Configuration 611
OSPFv3 Route Redistribution Summary 613

IPv6 Routes **614**

IPv6 Route Entry Configuration 614
IPv6 Route Table 616
IPv6 Route Preferences 617
Configured IPv6 Routes 619

Downloaded from www.Manualslib.com manuals search engine

11 Configuring Quality of Service

Quality of Service Overview **621**

Configuring Differentiated Services **622**

DiffServ Overview 622
Defining DiffServ 622
Diffserv Configuration 623
Class Configuration 624
Class Criteria 626
Policy Configuration 630
Policy Class Definition 633
Service Configuration 637
Service Detailed Statistics 638

Class of Service **639**

Mapping Table Configuration 640
Interface Configuration 644
Interface Queue Configuration 645

Auto VoIP **648**

Auto VoIP Global Configuration 648
Auto VoIP Interface Configuration 649

12 Configuring IP Multicast

Overview **651**

Multicast Global Configuration 652
Multicast Interface Configuration 655
Multicast Mroute Summary 656
Multicast Static Routes Configuration 658
Multicast Static Routes Summary 659
Multicast Admin Boundary Configuration 660
Multicast Admin Boundary Summary 662
Multicast Route Table 663

Multicast Listener Discovery **664**

MLD Global Configuration 664
MLD Routing Interface Configuration 665
MLD Routing Interface Summary 666
MLD Routing Interface Cache Information 668
MLD Routing Interface Source List Information 669

Downloaded from www.Manualslib.com manuals search engine

MLD Traffic 670
MLD Proxy Configuration 671
MLD Proxy Configuration Summary 673
Interface Membership Information 674
Interface Membership Information—Detailed 676

Distance Vector Multicast Routing Protocol 677
DVMRP Global Configuration 678
DVMRP Interface Configuration 679
DVMRP Configuration Summary 680
Next Hop Summary 683
Prune Summary 684
Route Summary 685

Internet Group Management Protocol 686
IGMP Global Configuration 687
Routing Interface 688
Proxy Interface 695

Protocol Independent Multicast-Dense Mode 701
PIM-DM Global Configuration 702
PIM-DM Global Status 703
PIM-DM Interface Configuration 704
PIM-DM Interface Summary 705
Candidate RP Configuration 707
Static RP Configuration 709
SSM Range Configuration 711
BSR Candidate Configuration 713
BSR Candidate Summary 714

Protocol Independent Multicast-Sparse Mode 714
PIM-SM Global Configuration 715
PIM-SM Global Status 718
PIM-SM Interface Configuration 719
PIM-SM Interface Summary 721
Component Summary 723
RP Set Summary 724
Candidate RP Summary 725
Static RP Configuration 726

Downloaded from www.Manualslib.com manuals search engine

13 Getting Help

Online Services 730
Automated Order-Status Service 731
Support Service 731

Dell Enterprise Training and Certification 731

Problems With Your Order 731

Product Information 732

Returning Items for Warranty Repair or Credit 732

Before You Call 732

Contacting Dell 734

Downloaded from www.Manualslib.com manuals search engine

1

Introduction

This section describes the switch user-configurable features. For a list of all features, see the software version release notes.

Note: Before proceeding, read the release notes for this product. You can download the release notes from the Dell Support website, **support.dell.com**.

The Dell™ PowerConnect™ M6348 is a Stackable Layer 3, Gigabit Ethernet modular switch for use in the Dell M1000e Chassis

The Dell™ PowerConnect™ M8024 is a non-Stackable Layer 3, 10 Gigabit Ethernet modular switch for use in the Dell M1000e Chassis.

The Dell™ PowerConnect™ M6220 is a Stackable Layer 3, Gigabit Ethernet modular switch for use in the Dell M1000e Chassis.

The topics covered in this section include:

- System Features
- Switching Features
- Routing Features
- IPv6
- Quality of Service Features
- Multicast Features
- CLI Documentation

Downloaded from www.Manualslib.com manuals search engine

System Features

sFlow

sFlow is the standard for monitoring high-speed switched and routed networks. sFlow technology is built into network equipment and gives complete visibility into network activity, enabling effective management and control of network resources.

CDP Interoperability

Allows the PowerConnect switch to interoperate with Cisco™ devices running CDP.

Industry Standard Discovery Protocol (ISDP) is a proprietary Layer 2 network protocol which inter-operates with Cisco network equipment and is used to share information between neighboring devices (routers, bridges, access servers, and switches).

Auto Config

Auto Config is a software feature which provides for the configuration of a switch automatically when the device is initialized and no configuration file is found on the switch. Auto Config is accomplished in three phases:

1. Configuration or assignment of an IP address for the device
2. Assignment of a TFTP server
3. Obtaining a configuration file for the device from the TFTP server

Captive Portal

Blocks clients from accessing the network until user verification has been established. Verification can be configured to allow access for both guest and authenticated users. Authenticated users must be validated against a database of authorized Captive Portal users before access is granted.

SNMP Alarms and Trap Logs

The system logs events with severity codes and timestamps. The events are sent as SNMP traps to a trap recipient list.

For information about SNMP Alarms and Traps, see "Defining SNTP Global Parameters."

Web Based Management

You can manage the system from any web browser. The switch contains an embedded web server that serves HTML pages you can use to monitor and configure the system.

Configuration File Download

The switch's configuration file includes both system-wide and port-specific device configuration data. You can display configuration files through command-line interface (CLI) commands.

For information about downloading configuration files, see "Downloading Files."

Downloaded from www.Manualslib.com manuals search engine

Software Download

Software download enables storage of backup firmware images. For information about downloading the software, see "Software Download and Reboot."

Trivial File Transfer Protocol (TFTP)

The PowerConnect M6220/M6348/M8024 switches support boot image, firmware, and configuration upload or download through TFTP.

Remote Monitoring (RMON)

RMON is a standard Management Information Base (MIB) that defines current and historical MAC-layer statistics and control objects, allowing real-time information to be captured across the entire network.

Simple Network Management Protocol (SNMP) Versions 1, 2, and 3

The system is fully manageable using a combination of MIB variables, whose combined values represent all facets of the system state, and the SNMP protocol to examine and possibly modify these values. SNMP v1/v2c/v3 over the UDP/IP transport protocol is supported.

Command Line Interface

Command Line Interface (CLI) syntax and semantics conform as much as possible to common industry practice. CLI is composed of mandatory and optional elements. Context-sensitive help provides format and value ranges allowed for current commands, and the CLI interpreter provides command and keyword completion.

Syslog

Syslog is a protocol that allows event notifications to be sent to a set of desired remote servers where they can be stored, examined, and acted upon.

For information about Syslog, see "Managing Logs."

SNTP

The Simple Network Time Protocol (SNTP) assures accurate network switch clock time synchronization up to the millisecond. Time synchronization is performed by a network SNTP server.

For more information about SNTP, see "Configuring SNTP Settings."

Simple Mode

Users with a privilege level of 15 can configure the switch to operate in normal mode or simple mode. By default, the switch operates in normal mode. When the PowerConnect M6220/M6348/M8024 Series is operating in simple mode, a limited number of features are available to configure. For features that are not available in simple mode, their administrative Web pages and CLI commands are unavailable.

For more information about Simple Mode, see "Setting the Operational Mode."

Downloaded from www.Manualslib.com manuals search engine

Port Aggregator

The Port Aggregator feature minimizes the administration required for managing the PowerConnect M6220/M6348/M8024. When the switch is operating in simple mode, the administrator can map internal ports to external ports without having to know anything about STP, VLANs, Link Aggregation or other L2/L3 protocols.

For more information configuring the Port Aggregator feature, see "Using the Port Aggregator Feature."

Switching Features

Low Power on Short Cables

For cables of different length, a different level of power back-off should be set for active link to achieve good level of signal and stable data transmit. Power back-off level is determined during the auto-negotiation phase. Users can configure or view the maximum length of cable that is connected to transceiver.

IPv6 Access Control Lists

An IPv6 ACL consists of a set of rules which are matched sequentially against a packet. When a packet meets the match criteria of a rule, the specified rule action (Permit/Deny) is taken and the additional rules are not checked for a match.

Access Control List (ACL) Outbound Support

Supports binding of an acl (IP, MAC, or IPV6) in outbound direction on physical, LAG, and VLAN interfaces

IP Source Guard (IPSG)

IP source guard (IPSG) is a security feature that filters IP packets based on the source ID. The source ID may either be source IP address or a source IP address source MAC address pair. IPSG is disabled by default.

DHCP Snooping

DHCP Snooping is a security feature that monitors DHCP messages between a DHCP client and DHCP server. It filters harmful DHCP messages and builds a bindings database of (MAC address, IP address, VLAN ID, port) tuples that are specified as authorized. DHCP snooping can be enabled globally and on specific VLANs. Ports within the VLAN can be configured to be trusted or untrusted. DHCP servers must be reached through trusted ports.

DHCP L2 Relay

Permits L3 Relay agent functionality in L2 switched networks.

Downloaded from www.Manualslib.com manuals search engine

Dynamic ARP Inspection

Dynamic ARP Inspection (DAI) is a security feature that rejects invalid and malicious ARP packets. The feature prevents a class of man-in-the-middle attacks, where an unfriendly station intercepts traffic for other stations by poisoning the ARP caches of its unsuspecting neighbors. The miscreant sends ARP requests or responses mapping another station's IP address to its own MAC address.

Dynamic ARP Inspection relies on DHCP Snooping.

MLD Snooping

In IPv4, Layer 2 switches can use IGMP Snooping to limit the flooding of multicast traffic by dynamically configuring Layer 2 interfaces so that multicast traffic is forwarded to only those interfaces associated with IP multicast address.

In IPv6, MLD snooping performs a similar function. With MLD snooping, IPv6 multicast data is selectively forwarded to a list of ports intended to receive the data (instead of being flooded to all of the ports in a VLAN). This list is constructed by snooping IPv6 multicast control packets.

IGMP Snooping

Internet Group Management Protocol (IGMP) Snooping is a feature that allows a switch to forward multicast traffic intelligently on the switch. Multicast IP traffic is traffic that is destined to a host group. Host groups are identified by class D IP addresses, which range from 224.0.0.0 to 239.255.255.255. Based on the IGMP query and report messages, the switch forwards traffic only to the ports that request the multicast traffic. This prevents the switch from broadcasting the traffic to all ports and possibly affecting network performance.

Port Mirroring

Port mirroring monitors and mirrors network traffic by forwarding copies of incoming and outgoing packets from up to four source ports to a monitoring port.

Broadcast Storm Control

When Layer 2 frames are forwarded, broadcast, unknown unicast, and multicast frames are flooded to all ports on the relevant virtual local area network (VLAN). The flooding occupies bandwidth, and loads all nodes connected on all ports. Storm control limits the amount of broadcast, unknown unicast, and multicast frames accepted and forwarded by the switch.

Downloaded from www.Manualslib.com manuals search engine

Port-Based Features

Jumbo Frames Support

Jumbo frames enable transporting identical data in fewer frames to ensure less overhead, lower processing time, and fewer interrupts.

Auto-MDI/MDIX Support

Your switch supports auto-detection between crossed and straight-through cables.

Media-Dependent Interface (MDI) is the standard wiring for end stations, and the standard wiring for hubs and switches is known as Media-Dependent Interface with Crossover (MDIX).

Auto Negotiation

Auto negotiation allows the switch to advertise modes of operation. The auto negotiation function provides the means to exchange information between two switches that share a point-to-point link segment, and to automatically configure both switches to take maximum advantage of their transmission capabilities.

The PowerConnect M6220/M6348/M8024 enhances auto negotiation by providing port advertisement. Port advertisement allows the system administrator to configure the port speeds advertised.

For information about auto negotiation, see "Port Configuration" or "LAG Configuration."

Flow Control Support (IEEE 802.3x)

Flow control enables lower speed switches to communicate with higher speed switches by requesting that the higher speed switch refrains from sending packets. Transmissions are temporarily halted to prevent buffer overflows.

For information about configuring flow control for ports or LAGs, see "Port Configuration" or "LAG Configuration."

Head of Line Blocking Prevention

Head of Line (HOL) blocking prevention prevents traffic delays and frame loss caused by traffic competing for the same egress port resources. HOL blocking queues packets, and the packets at the head of the queue are forwarded before packets at the end of the queue.

Back Pressure Support

On half-duplex links, a receiver may prevent buffer overflows by occupying the link so that it is unavailable for additional traffic.

Downloaded from www.Manualslib.com manuals search engine

Alternate Store and Forward (ASF)

The Alternate Store and Forward (ASF) feature reduces latency for large packets. When ASF is enabled, the memory management unit (MMU) can forward a packet to the egress port before it has been entirely received on the Cell Buffer Pool (CBP) memory. AFS, which is also known as cut-through mode, is configurable through the command-line interface. For information about how to configure the AFS feature, see the *CLI Reference Guide*, which is located on the Dell Support website at **www.support.dell.com/manuals**.

Link Dependency Features

The link dependency feature provides the ability to enable or disable one or more ports based on the state of the link of one or more ports.

For information about Link Dependency, see "Creating Link Dependencies."

Virtual Local Area Network Supported Features

VLAN Support

VLANs are collections of switching ports that comprise a single broadcast domain. Packets are classified as belonging to a VLAN based on either the VLAN tag or a combination of the ingress port and packet contents. Packets sharing common attributes can be groups in the same VLAN.

For information about configuring VLANs, see "Configuring VLANs."

Port-Based VLANs

Port-based VLANs classify incoming packets to VLANs based on their ingress port. When a port uses 802.1X port authentication, packets can be assigned to a VLAN based on the result of the 802.1X authentication a client uses when it accesses the switch. This feature is useful for assigning traffic to Guest VLANs or Voice VLANs.

For information about configuring VLANs, see "Configuring VLANs."

IEEE 802.1v Protocol-Based VLANs

VLAN classification rules are defined on data-link layer (Layer 2) protocol identification. Protocol-based VLANs are used for isolating Layer 2 traffic for differing Layer 3 protocols.

For information about defining Protocol-Based VLANs, see "Protocol Group."

Full 802.1Q VLAN Tagging Compliance

IEEE 802.1Q defines an architecture for virtual bridged LANs, the services provided in VLANs, and the protocols and algorithms involved in the provision of these services.

Downloaded from www.Manualslib.com manuals search engine

GVRP Support

GARP VLAN Registration Protocol (GVRP) provides IEEE 802.1Q-compliant VLAN pruning and dynamic VLAN creation on 802.1Q trunk ports. When GVRP is enabled, the switch registers and propagates VLAN membership on all ports that are part of the active spanning tree protocol topology.

For information about configuring GVRP, see "GVRP Parameters."

Protected Ports (Private VLAN Edge)

Private VLAN Edge (PVE) ports are a Layer 2 security feature that provides port-based security between ports that are members of the same VLAN. It is an extension of the common VLAN. Traffic from protected ports is sent only to the uplink ports and cannot be sent to other ports within the VLAN.

Subnet-based VLAN

This feature allows incoming untagged packets to be assigned to a VLAN and traffic class based on the source IP address of the packet.

For information about configuring Subnet-based VLANs, see "Bind IP Subnet to VLAN."

MAC-based VLAN

This feature allows incoming untagged packets to be assigned to a VLAN and traffic class based on the source MAC address of the packet.

For information about configuring MAC-based VLANs, see "Bind MAC to VLAN."

Double VLANs

The Double VLAN feature allows the use of a second tag on network traffic. The additional tag helps differentiate between customers in the Metropolitan Area Networks (MAN) while preserving individual customer's VLAN identification when they enter their own 802.1Q domain.

Protocol-based VLANs

In a protocol-based VLAN, traffic is bridged through specified ports based on the VLAN's protocol. User-defined packet filters determine if a particular packet belongs to a particular VLAN. Protocol-based VLANs are most often used in situations where network segments contain hosts running multiple protocols.

Downloaded from www.Manualslib.com manuals search engine

Spanning Tree Protocol Features

Spanning Tree now supports IEEE802.1Q-2005

This version of the IEEE Multiple Spanning Tree Protocol corrects problems associated with the previous version, provides for faster transition-to-forwarding, and incorporates new features for a port (restricted role and restricted TCN).

Spanning Tree Enhancements

- **Loop Guard** — This feature prevents a port from erroneously transitioning from blocking state to forwarding when the port stops receiving BPDUs. The port is marked as being in loop-inconsistent state. In this state, the port does not forward packets. The possible values are Enable or Disable.
- **TCN Guard** — Enabling the TCN Guard feature restricts the port from propagating any topology change information received through that port. This means that even if a port receives a BPDU with the topology change flag set to true, the port will not flush its MAC address table and send out a BPDU with a topology change flag set to true.
- **Auto Edge** — Enabling the Auto Edge feature allows the port to become an edge port if it does not see BPDUs for some duration.
- **BPDU Filter** — When enabled, this feature filters the BPDU traffic on this port when STP is enabled on this port.
- **BPDU Flood** — When enabled, the BPDU Flood feature floods the BPDU traffic arriving on this port when STP is disabled on this port.

Spanning Tree Protocol (STP) per Switch

802.1d STP is a standard requirement of Layer 2 switches that allows bridges to automatically prevent and resolve L2 forwarding loops.

For information about configuring Spanning Tree Protocol, see "Configuring the Spanning Tree Protocol."

IEEE 802.1w Rapid Spanning Tree

Rapid Spanning Tree Protocol (RSTP) detects and uses network topologies to enable faster spanning tree convergence after a topology change, without creating forwarding loops.

For information about configuring Rapid Spanning Tree Protocol, see "Rapid Spanning Tree."

Multiple Spanning Tree

Multiple Spanning Tree (MSTP) operation maps VLANs to spanning tree instances. Packets assigned to various VLANs are transmitted along different paths within MSTP Regions (MST Regions). Regions are one or more interconnected MSTP bridges with identical MSTP settings. The MSTP standard lets administrators assign VLAN traffic to unique paths.

For information about configuring Multiple Spanning Tree, see "MSTP Settings."

Downloaded from www.Manualslib.com manuals search engine

Spanning Tree Root Guard

Spanning Tree Root Guard is used to prevent the root of a Spanning Tree instance from changing unexpectedly. The priority of a Bridge ID can be set to zero but another Bridge ID with a lower mac address could also set its priority to zero and take over root.

Bridge Protocol Data Unit Guard

Spanning Tree BPDU Guard is used to disable the port in case a new device tries to enter the already existing topology of STP. Thus devices, which were originally not a part of STP, are not allowed to influence the STP topology.

Link Aggregation Features

Link Aggregation

Up to eight ports can combine to form a single Link Aggregated Group (LAG). This enables fault tolerance protection from physical link disruption, higher bandwidth connections and improved bandwidth granularity.

A LAG is composed of ports of the same speed, set to full-duplex operation.

For information about configuring LAGs, see "LAG Configuration."

Link Aggregation and LACP

Link Aggregate Control Protocol (LACP) uses peer exchanges across links to determine, on an ongoing basis, the aggregation capability of various links, and continuously provides the maximum level of aggregation capability achievable between a given pair of systems. LACP automatically determines, configures, binds, and monitors the binding of ports to aggregators within the system.

For information about LACP, see "LACP Parameters."

Downloaded from www.Manualslib.com manuals search engine

Routing Features

VLAN Routing

The PowerConnect M6220/M8024/M6348 software supports VLAN routing. You can also configure the software to allow traffic on a VLAN to be treated as if the VLAN were a router port.

Routing Information Protocol (RIP)

The route configuration and route preference features have the following changes:

- You can configure static reject routes (see Static Reject Routes).
- The default values for route preferences have changed.
- OSPF Type-1 and OSPF Type-2 routes are now classified as OSPF External routes.

OSPF Configuration

The Maximum Paths field allows OSPF to report a maximum of 4 paths for a given destination.

The following fields have been added for OSPF configuration options:

- Opaque LSA Status
- AS_OPAQUE LSA Count
- AS_OPAQUE LSA Checksum
- External LSDB Limit
- AutoCost Reference Bandwidth
- Default Passive Setting
- Stub Area Type of Service
- NSSA Information

The **OSPF Link State Database** page has been updated to display external LSDB table information and AS opaque LSDB table information (in addition to OSPF link state information).

IP Configuration

The switch IP configuration settings have been enhanced to allow you to enable or disable the generation of the following types of ICMP messages:

- ICMP Echo Replies
- ICMP Redirects
- ICMP Rate Limit Interval
- ICMP Rate Limit Burst Size

Downloaded from www.Manualslib.com manuals search engine

IP Interface Configuration

IP interface configuration includes the ability to configure the bandwidth, Destination Unreachable messages, and ICMP Redirect messages.

IP Helper

Provides the ability to relay various protocols to servers on a different subnet.

VRRP Route Interface Tracking

Extends the capability of the Virtual Router Redundancy Protocol (VRRP) to allow tracking of specific route/interface IP state within the router that can alter the priority level of a virtual router for a VRRP group.

The exception to this is, if that VRRP group is the IP address owner, its priority is fixed at 255 and can not be reduced through tracking process.

MAC Address Supported Features

MAC Address Support

The switch supports up to 8K Media Access Control (MAC) addresses and reserves two MAC addresses for system use.

Self-Learning MAC Addresses

The switch enables MAC addresses to be automatically learned from incoming packets.

Automatic Aging for MAC Addresses

MAC addresses that have not seen any traffic for a given period are aged out, which prevents the bridging table from overflowing.

For information about configuring the MAC Address age-out period, see "Dynamic Address Table."

Static MAC Entries

User-defined MAC entries are stored in the Bridging Table with the self-learned addresses.

For information about configuring the static MAC addresses, see "Static Address Table."

VLAN-Aware MAC-based Switching

Packets arriving from an unknown source address are sent to the CPU and added to the Hardware Table. Future packets addressed to or from this address are more efficiently forwarded.

Downloaded from www.Manualslib.com manuals search engine

MAC Multicast Support

Multicast service is a limited broadcast service that allows one-to-many and many-to-many connections. In Layer 2 multicast services, a single frame addressed to a specific multicast address is received, and copies of the frame to be transmitted on each relevant port are created.

For information about configuring MAC Multicast Support, see "Managing Multicast Support."

IPv4 Routing Features

Address Resolution Protocol

The PowerConnect M6220/M6348/M8024 uses the ARP protocol to associate a layer 2 MAC address with a layer 3 IPv4 address. Additionally, the administrator can statically add entries in to the ARP table.

Open Shortest Path First

The Open Shortest Path First (OSPF) Routing protocol defines two area types: regular OSPF area and OSPF stub area. OSPF internal and external route information may be propagated throughout the regular OSPF area; it is capable of supporting transit traffic and virtual links. OSPF stub areas do not receive external route information; the motivation to configure stub areas is to limit the size of the area database for those routers that have limited resources.

BOOTP/DHCP Relay Agent

The BootP protocol allows a device to solicit and receive configuration data and parameters from a suitable server. DHCP is an extension to BootP allowing additional setup parameters to be received from a network server upon system startup. Notably, while BootP stops operating once an IP address is obtained, DHCP service is an on-going process. For example, the IP address assigned to the system has a 'lease time' that may expire, and can be renewed on the fly.

Routing Information Protocol

The routing protocol used within an autonomous Internet system is referred to as an interior gateway protocol (IGP). RIP is an IGP that is designed to work with moderate-size networks.

Virtual Routing Redundancy Protocol

Virtual Routing Redundancy Protocol (VRRP) is used to provide hosts with redundant routers in the network topology without any need for the hosts to reconfigure or know that there are multiple routers.

Downloaded from www.Manualslib.com manuals search engine

IPv6 Routing Features

IPv6 6 to 4 Auto Tunnels

Automatically formed IPv4 6 to 4 tunnels for carrying IPv6 traffic. The automatic tunnel IPv4 destination address is derived from the 6 to 4 IPv6 address of the tunnel nexthop. There is support the functionality of a 6 to 4 border router that connects a 6 to 4 site to a 6 to 4 domain. It sends/receives tunneled traffic from routers in a 6 to 4 domain that includes other 6 to 4 border routers and 6 to 4 relay routers.

DHCPv6

DHCPv6 incorporates the notion of the "stateless" server, where DHCPv6 is not used for IP address assignment to a client, rather it only provides other networking information such as DNS, Network Time Protocol (NTP), and/or Session Initiation Protocol (SIP) information.

OSPFv3

OSPFv3 provides a routing protocol for IPv6 networking. OSPFv3 is a new routing component based on the OSPF version 2 component. In dual stack IPv6, you can configure and use both OSPF and OSPFv3 components.

IPv6 Routes

Since IP4 and IPV6 can coexist on a network, the router on such a network needs to forward both traffic types. Given this coexistence, the PowerConnect M6220/M6348/M8024 maintains two routing tables, rto and rto6, which are both capable of forwarding over the same set of interfaces. IPV6 interfaces are managed in a manner similar to IPV4 interfaces.

IPv6

IPv6 Route Configuration Enhancements

The route configuration and route preference features have the following changes:

You can configure static reject routes.

The default values for route preferences have changed as follows:

- OSPFv3 Intra — 110
- OSPFv3 Inter — 110
- OSPFv3 External — 110

OSPF Type-1 and OSPF Type-2 routes are now classified as OSPF External routes.

Downloaded from www.Manualslib.com manuals search engine

OSPFv3

The OSPFv3 Configuration page has been updated with the following changes:

- AutoCost Reference Bandwidth field
- Default Passive Setting field
- Maximum Paths increased from 2 to 4
- Passive Mode field

Quality of Service Features

Voice VLAN

The Voice VLAN feature enables switch ports to carry voice traffic with defined priority. The priority level enables the separation of voice and data traffic coming onto the port. A primary benefit of using Voice VLAN is to ensure that the sound quality of an IP phone is safeguarded from deteriorating when the data traffic on the port is high. The system uses the source MAC address of the traffic traveling through the port to identify the IP phone data flow.

Auto VoIP

Provides ease of use for the user in setting up VoIP for IP phones on a switch. This is accomplished by enabling a VoIP profile that a user can select on a per port basis.

Class of Service Rate Limiting

The Class of Service interface configuration feature has been enhanced to allow outbound rate limiting on specified ports.

Differentiated Services IPv6 Support

Extends the existing QoS ACL and DiffServ functionality by providing support for IPv6 packet classification. Ethernet IPv6 packets are distinguished from IPv4 packets by a unique Ethertype value (all IPv6 classifiers include the Ethertype field).

Quality of Service (QoS) Support

To overcome unpredictable network traffic and optimize performance, you can apply Quality of Service (QoS) throughout the network. QoS ensures that the network traffic is prioritized according to a specific criteria. Your switch supports two types of QoS: Differentiated Services and Class of Service.

- The QoS Differentiated Services (DiffServ) feature allows traffic to be classified into streams and given certain QoS treatment in accordance with defined per-hop behaviors.
- The Class Of Service (CoS) queueing feature lets you directly configure certain aspects of switch queuing. This provides the desired QoS behavior for different types of network traffic when the complexities of DiffServ are not required.

Downloaded from www.Manualslib.com manuals search engine

Multicast Features

IPv4 Multicast Features

Updated IPv4 Multicast Routing Support

The Multicast package code has been extensively re-engineered and furnished with the following:

- PIM-DM advanced to RFC 3973
- PIM-SM advanced to RFC 4601, pim-sm-bsr-05, draft-ietf-pim-mib-v2-03
- DVMRP advanced to draft-ietf-idmr-dvmrp-v3-10.txt, draft-ietf-idmr-dvmrp-mib-11.txt

Distance Vector Multicast Routing Protocol

Distance Vector Multicast Routing Protocol (DVMRP) exchanges probe packets with all DVMRP-enabled routers, establishing two way neighboring relationships and building a neighbor table. It exchanges report packets and creates a unicast topology table, which is used to build the multicast routing table. This multicast route table is then used to route the multicast packets.

Internet Group Management Protocol

The Internet Group Management Protocol (IGMP) is used by IPv4 systems (hosts and routers) to report their IP multicast group memberships to any neighboring multicast routers. The PowerConnect M6220/M6348/M8024 performs the "multicast router part" of the IGMP protocol, which means it collects the membership information needed by the active multicast routing.

Protocol Independent Multicast-Dense Mode

Protocol Independent Multicast (PIM) is a standard multicast routing protocol that provides scalable inter-domain multicast routing across the Internet, independent of the mechanisms provided by any particular unicast routing protocol. The Protocol Independent Multicast-Dense Mode (PIM-DM) protocol uses an existing Unicast routing table and a Join/Prune/Graft mechanism to build a tree. PIM-DM creates source-based shortest-path distribution trees, making use of reverse path forwarding (RPF).

Protocol Independent Multicast-Sparse Mode

Protocol Independent Multicast-Sparse Mode (PIM-SM) is used to efficiently route multicast traffic to multicast groups that may span wide area networks, and where bandwidth is a constraint. PIM-SM uses shared trees by default and implements source-based trees for efficiency. This data threshold rate is used to toggle between trees.

Downloaded from www.Manualslib.com manuals search engine

IPv6 Multicast Features

Protocol Independent Multicast IPv6 Support

PIM-DM and PIM-SM support IPv6 routes.

MLD/MLDv2 (RFC2710/RFC3810)

MLD is used by IPv6 systems (listeners and routers) to report their IP multicast addresses memberships to any neighboring multicast routers. The implementation of MLD v2 is backward compatible with MLD v1.

MLD protocol enables the IPv6 router to discover the presence of multicast listeners, the nodes that want to receive the multicast data packets, on its directly attached interfaces. The protocol specifically discovers which multicast addresses are of interest to its neighboring nodes and provides this information to the multicast routing protocol that make the decision on the flow of the multicast data packets.

Security Features

Access Control Lists (ACL)

Access Control Lists (ACLs) ensure that only authorized users have access to specific resources while blocking off any unwarranted attempts to reach network resources. ACLs are used to provide traffic flow control, restrict contents of routing updates, decide which types of traffic are forwarded or blocked, and above all provide security for the network.

For information about defining ACLs, see "IP ACL Configuration" and "MAC ACL Configuration."

Dot1x Authentication (802.1x)

Dot1x authentication enables the authentication of system users through an external server. Only authenticated and approved system users can transmit and receive data. Supplicants are authenticated through the Remote Authentication Dial In User Service (RADIUS) server using the Extensible Authentication Protocol (EAP). Also supported are PEAP, EAP-TTL, EAP-TTLS, and EAP-TLS. MAC-based authentication allows multiple supplicants connected to the same port to each authenticate individually. For example, a system attached to the port might be required to authenticate in order to gain access to the network, while a VoIP phone might not need to authenticate in order to send voice traffic through the port.

For information about enabling and configuring 802.1X port authentication, see "Dot1x Authentication."

Locked Port Support

The locked port feature limits access on a port to users with specific MAC addresses. These addresses are manually defined or learned on that port. When a frame is seen on a locked port, and the frame source MAC address is not tied to that port, the protection mechanism is invoked.

For information about enabling locked port security, see "Port Security."

Downloaded from www.Manualslib.com manuals search engine

Password Management Security

Password management provides increased network security and improved password control. Passwords for SSH, Telnet, HTTP, HTTPS, and SNMP access are assigned security features.

For more information about password management, see "Password Management."

TACACS+

TACACS+ provides centralized security for validation of users accessing the switch. TACACS+ provides a centralized user management system, while still retaining consistency with RADIUS and other authentication processes.

RADIUS Client

RADIUS is a client/server-based protocol in which the server maintains a user database that contains user authentication information, such as user name, password, and accounting information.

SSH/SSL

Secure Shell (SSH) is a protocol that provides a secure, remote connection to a device. This connection provides functionality that is similar to an inbound telnet connection.

Secure Sockets Layer (SSL) protocol provides a means of abstracting an encrypted connection between two stations. Once established, such a connection is virtually no different to use than an unsecured connection.

CLI Documentation

Another resource for the PowerConnect M6220/M6348/M8024 is the *CLI Reference Guide,* which is located on the Dell Support website at **www.support.dell.com**. It provides information about the command-line interface (CLI) commands used to configure and manage the switch. The document provides in-depth CLI descriptions, syntax, default values, and examples.

Downloaded from www.Manualslib.com manuals search engine

2

Using Dell™ OpenManage™ Switch Administrator

The topics covered in this section include:

- Setting the IP Address of the Switch
- Starting the Application
- Understanding the Interface
- Using the Switch Administrator Buttons
- Defining Fields
- Accessing the Switch Through the CLI
- Using the CLI

Downloaded from www.Manualslib.com manuals search engine

Setting the IP Address of the Switch

Two methods for setting the IP address are to use DHCP or to statically assign the address. See the the section titled "Accessing the Switch Through the CLI" on page 41 to start the CLI.

Verifying the Out-of-Band (OOB) IP Address

Using the **show ip interface out-of-band** command, verify that the OOB interface has an IP address.

```
console#show ip interface out-of-band


IP Address..................................... 10.27.22.168
Subnet Mask.................................... 255.255.255.0
Default Gateway................................ 10.27.22.1
ServPort Configured Protocol Current........... DHCP
Burned In MAC Address......................... 0063.4802.0011


console#
```

If DHCP is not available on your network, set a static IP address.

Setting a Static IP Address

1. Type **`enable`** at the console> prompt, and press <Enter>.
2. At the console# prompt, type **`config`** and press <Enter>.
3. Type **`interface out-of-band.`**
4. To configure an ip address of 10.256.24.64 and a netmask of 255.255.248.0, type the following:

   `ip address 10.256.24.64 255.255.248.0`
5. Type `exit`.

Downloaded from www.Manualslib.com manuals search engine

Starting the Application

1. Open a web browser.
2. Enter the switch's IP address (as defined in the CLI) or the out-of-band IP address in the address bar and press <Enter>.

   For information about assigning an IP address to a switch, see "Configuration Overview."
3. When the **Login** window displays, enter a user name and password.

   Note: The switch is not configured with a default password, and you can configure the switch without entering a password when you connect to the CLI by using the console port. Passwords are both case sensitive and alpha-numeric. For information about recovering a lost password, see "Password Recovery Procedure."
4. Click **OK**.
5. The **Dell OpenManage Switch Administrator** home page displays.

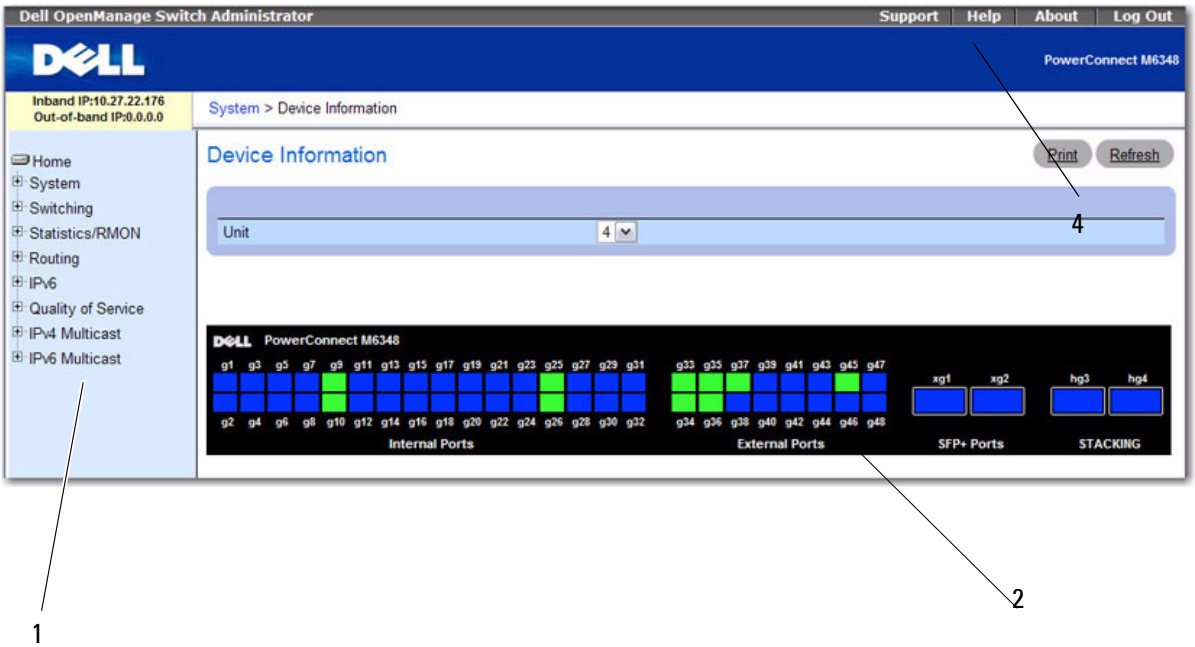
Understanding the Interface

The home page contains the following views:

- **Tree view** — Located on the left side of the home page, the tree view provides an expandable view of features and their components.
- **Device view** — Located on the right side of the home page, the device view is used to display such things as a view of the device, an information or table area, and/or configuration instructions.

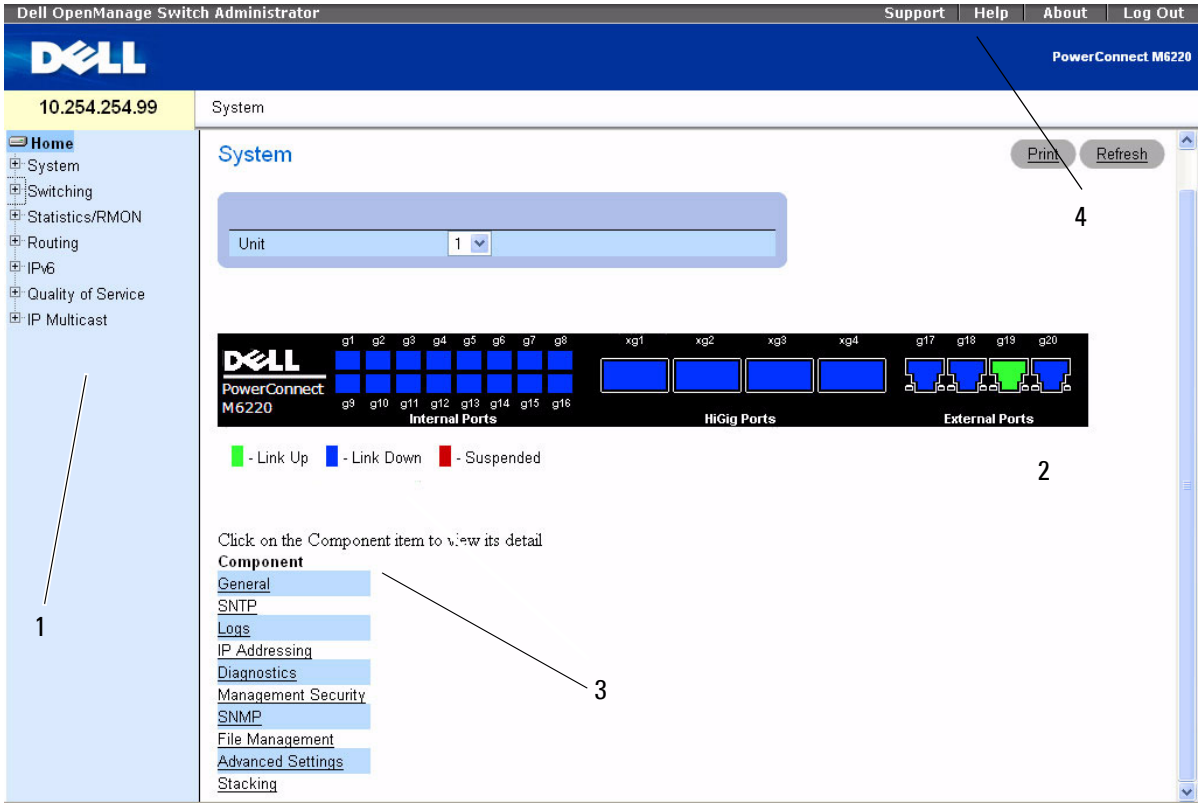
Downloaded from www.Manualslib.com manuals search engine

Figure 2-1. Switch Administrator Components PowerConnect M6348



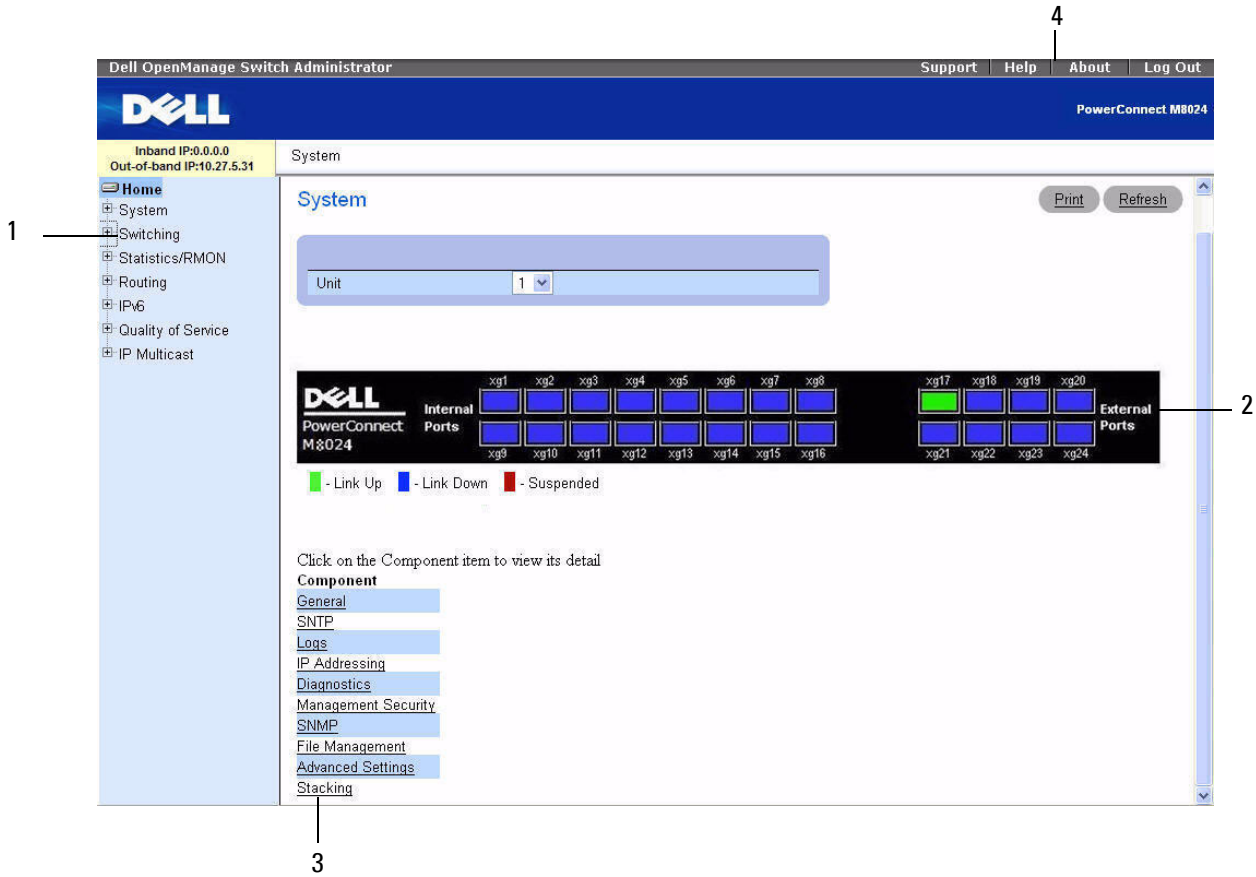
Downloaded from www.Manualslib.com manuals search engine

Figure 2-2. Switch Administrator Components PowerConnect M6220



Downloaded from www.Manualslib.com manuals search engine

Figure 2-3. Switch Administrator Components PowerConnect M8024



Downloaded from www.Manualslib.com manuals search engine

Table 2-1 lists the interface components with their corresponding numbers.

Table 2-1. Interface Components

Component	Name
1.	The tree view contains a list of various device features. The branches in the tree view can be expanded to view all the components under a specific feature, or retracted to hide the feature's components. By dragging the vertical bar to the right, you can expand the tree area to view a full name of a component.
2.	The device view provides information about device ports, current configuration and status, table information, and feature components. The port coloring indicates if a port is currently active. Green indicates the port is enabled, red indicates that an error has occurred on the port, and blue indicates that the link is disabled. **Note:** The LED status does not appear in the device view. You can only determine LED status by looking at the actual switch. For information about LEDs, see "PowerConnect LED Definitions." Depending on which option you select, the area at the bottom of the device view displays other device information and/or dialogs for configuring parameters.
3.	The components list contains a list of feature components. You can also view components by expanding a feature in the tree view.
4.	The information buttons provide access to information about the switch and access to Dell Support. For more information, see "Information Buttons."

Downloaded from www.Manualslib.com manuals search engine

Using the Switch Administrator Buttons

Information Buttons

Table 2-2. Information Buttons

Button	Description
Support	Opens the Dell Support page at **support.dell.com**
Help	Online help that contains information to assist in configuring and managing the switch. The online help pages are context sensitive. For example, if the **IP Addressing** page is open, the help topic for that page displays if you click **Help**.
About	Contains the version and build number and Dell copyright information.
Log Out	Logs out of the application.

Device Management Buttons

Table 2-3. Device Management Buttons

Button	Description
Apply Changes	Applies set changes to the device.
Add	Adds information to tables or dialogs.
Telnet	Starts a Telnet session.
Query	Queries tables.
Show All	Displays the device tables.
Left arrow/Right arrow	Moves information between lists.
Refresh	Refreshes device information.
Reset All Counters	Clears statistic counters.
Print	Prints the **Network Management System** page and/or table information.
Draw	Creates statistics charts on-the-fly.

Downloaded from www.Manualslib.com manuals search engine

Check Boxes

Table 2-4. Check Boxes

Check Box Type	Description
Add	Hyperlink that takes you to a configuration page.
Remove	Removes the selected item.
General selection	To enable a configuration item, i.e., adjust sensitivity of log files, select match criteria for diffserv, select ACL rule parameters.

Defining Fields

User-defined fields can contain 1–159 characters, unless otherwise noted on the Dell OpenManage Switch Administrator Web page.

All characters may be used except for the following:

- \
- /
- :
- *
- ?
- <
- >
- |

Accessing the Switch Through the CLI

The switch can be managed over a direct connection to the console port or through a Telnet connection.

If you are managing a stack, ensure the serial interface cable is attached to the Master switch of the stack.

Using the CLI is similar to entering commands on a Linux system. If access is through a Telnet connection, ensure the device has an IP address defined and that the workstation used to access the device is connected to the device prior to using CLI commands.

For information about configuring an initial IP Address, see "Configuration Overview."

Downloaded from www.Manualslib.com manuals search engine

Console Connection

1. Turn on the switch and wait until the startup is complete.
2. If the admin has not configured a login authentication method, then the `console>` prompt displays when the switch boots up. Otherwise, the user is presented with the `User:` login prompt.

   Note: The following steps assume that the admin user and password is configured on the system.

3. Type `admin` at the prompt, and press <Enter>.

   The `Password`: prompt now displays.

4. Enter the password, which displays as asterisks (*).

   The `console#` prompt now displays.

5. Configure the device and enter the necessary commands to complete the required tasks.
6. When finished, exit the session with the **`quit`** or **`exit`** command.

Telnet Connection

Telnet is a terminal emulation TCP/IP protocol. ASCII terminals can be virtually connected to the local device through a TCP/IP protocol network. Telnet is an alternative to a local login terminal where a remote login is required.

Your switch supports up to four simultaneous Telnet sessions. All CLI commands can be used over a telnet session.

Using the CLI

Command Mode Overview

The CLI is divided into command modes. Each command mode has a specific command set. Entering a question mark at the console prompt displays a list of commands available for that particular command mode.

In each mode, a specific command is used to navigate from one command mode to another.

During the CLI session initialization, the CLI mode is the User EXEC mode. Only a limited subset of commands are available in the User EXEC mode. This level is reserved for tasks that do not change the switch configuration and is used to access configuration sub-systems. Privileged EXEC mode may require a password if the enable password is configured. See "Security Management and Password Configuration" on page 83 for more information on setting up enable passwords.

The Privileged EXEC mode provides access to the device global configuration. For specific global configurations within the device, enter the next level, Global Configuration mode. A password is not required.

The Global Configuration mode manages the device configuration on a global level.

Downloaded from www.Manualslib.com manuals search engine

The Interface Configuration mode configures the device at the physical interface level. Interface commands, which require subcommands, have another level called the Subinterface Configuration mode.

User EXEC Mode

The user EXEC level prompt consists of the host name followed by the angle bracket (>). For example:

```
console>
```

Note: The default host name is `console` unless it has been modified during initial configuration.

The user EXEC commands permit connecting to remote devices, changing terminal settings on a temporary basis, performing basic tests, and listing system information.

To list the user EXEC commands, enter a question mark at the command prompt.

Privileged EXEC Mode

Privileged access can be protected to prevent unauthorized access and ensure operating parameters. Passwords are case-sensitive, and each character of the password displays on screen as an asterisk.

To access and list the Privileged EXEC Mode commands:

1. At the prompt type `enable` and press <Enter>.
2. If a password prompt displays, enter the password and press <Enter>.

   The Privileged EXEC mode prompt displays as the device host name followed by #. For example:

   ```
   console#
   ```

3. To list the Privileged EXEC commands, type a question mark at the command prompt.
4. To return from Privileged EXEC Mode to User EXEC Mode, type the `exit` command or press <Ctrl><Z> keys.

The following example illustrates accessing privileged EXEC mode and then returning to the User EXEC mode:

```
console>enable
Enter Password: ******
console#
console#exit
console>
```

Use the `exit` command to move back to a previous mode. For example, you can move from Interface Configuration mode to Global Configuration mode, and from Global Configuration mode to Privileged EXEC mode.

Downloaded from www.Manualslib.com manuals search engine

Global Configuration Mode

Global Configuration commands apply to system features, rather than to a specific protocol or interface.

To access Global Configuration mode:

1. At the Privileged EXEC Mode prompt, type `configure` and press <Enter>. The Global Configuration Mode displays as the device host name, followed by (config) and the number sign #.

   ```
   console(config)#
   ```

2. To list the Global Configuration commands, enter a question mark at the command prompt.
3. To return from Global Configuration mode to Privileged EXEC mode, type the `exit` command or use the <Ctrl><Z> command.

The following example illustrates how to access *Global Configuration Mode* and return to the *Privileged EXEC Mode*:

```
console#
console#configure
console(config)#exit
console#
```

Interface Configuration Mode

Interface configuration commands modify specific IP interface settings, including bridge-group, description, and so forth. The Interface Configuration modes are:

- **VLAN** — Contains commands to create and configure a VLAN as a whole, for example, to create a VLAN and apply an IP address to the VLAN.
- **Port Channel** — Contains commands for configuring Link Aggregation Groups (LAG).
- **Ethernet** — Contains commands for managing Ethernet port configuration.
- **Loopback**—Contains commands for managing Loopback interface configuration.
- **Tunnel**—Contains commands for managing Tunnel interface configuration.
- **Out-of-band**—Contains commands for configuring the out-of-band interface.

Downloaded from www.Manualslib.com manuals search engine

3

Cable and Port Information

Overview

This section describes the switch's physical interfaces and provides information about cable connections.

Stations are connected to the switch's ports through the physical interface ports on the front panel. For each station, the appropriate mode (Half/Full Duplex, Auto) is set.

The topics covered in this section include:

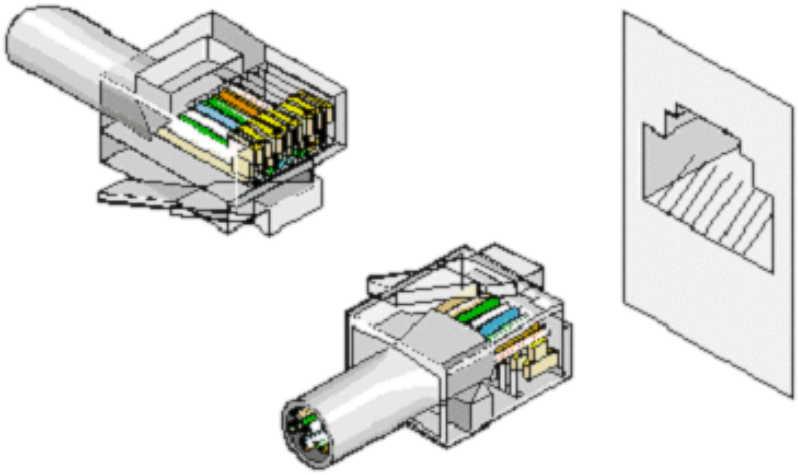
- Ethernet Interface
- Bay 1 and Bay 2 Interfaces (M6220 and M8024)
- Serial Cable Connection
- Power Connection

Downloaded from www.Manualslib.com manuals search engine

Ethernet Interface

The switching port can connect to stations wired in standard RJ-45 Ethernet station mode using straight cables. Transmission devices connected to each other use crossed cables. Figure 3-1 illustrates the RJ-45 connector.

Figure 3-1. RJ-45 Connector



Downloaded from www.Manualslib.com manuals search engine

Bay 1 and Bay 2 Interfaces (M6220 and M8024)

The PowerConnect M6220 supports dual 10G slot interfaces. These interfaces can operate at 10 Gbps when supporting optional 10GE modules, or 12 Gbps (top slot only) when supporting a stacking module. Figure 3-2 illustrates the 10G slots.

The Dell™ PowerConnect™ M8024 supports dual 10 Gb slot interfaces. These interfaces can operate at 10 Gbps when supporting optional SFP+ or CX4 modules. Figure 3-3 illustrates the 10 Gb slots.

Figure 3-2. Bay 1 and Bay 2 PowerConnect M6220 Series 10 Gb Slots

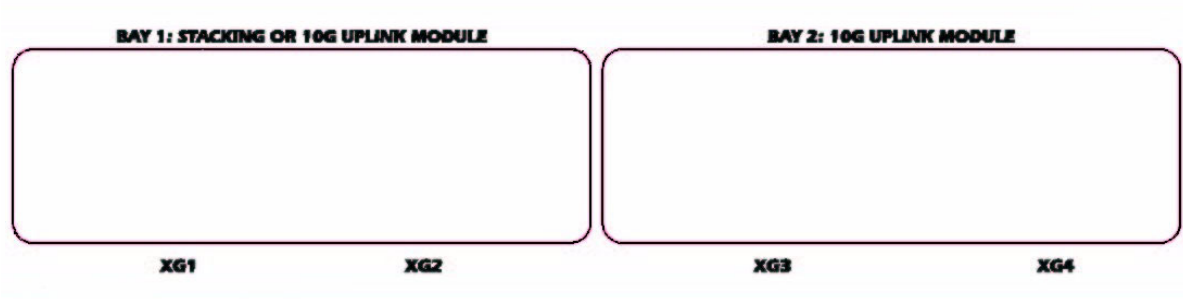
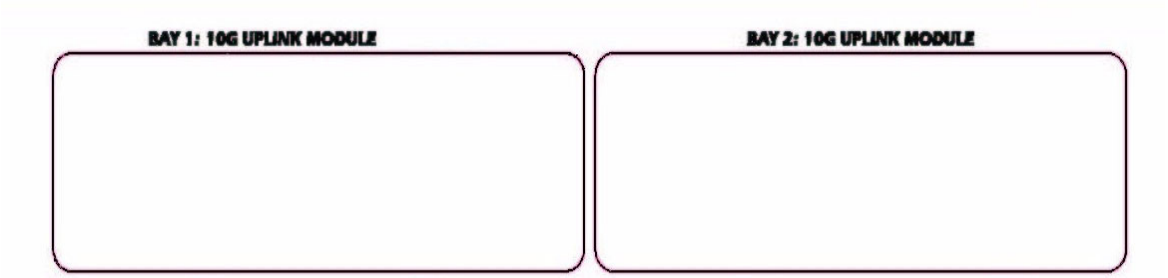


Figure 3-3. Bay 1 and Bay 2 PowerConnect M8024 10 Gb Slots



Downloaded from www.Manualslib.com manuals search engine

Serial Cable Connection

You can use the suppled USB Type A to DB9a serial cable (null-modem) to connect the switch to a terminal for initial setup and configuration (You can also use a computer running terminal emulation software.). The switch's serial cable is a USB type A to female DB-9 crossover cable (see Figure 3-4).

Figure 3-4. Serial Connectors

Connecting the Switch to a Terminal

1. Connect the serial cable to the terminal (console) ASCII DTE RS-232.
2. Connect the serial cable to the switch's serial port.
3. If you are configuring a stack, connect the interface cable to the serial port of the Master switch.

For more information about connecting to the Dell™ PowerConnect™ M6220 serial port, see the *M6220 Series Stackable Switches Getting Started Guide*.

For more information about connecting to the PowerConnect M8024 serial port, see the *PowerConnect M8024 Switch Getting Started Guide,* which is located on the Dell Support website at **www.support.dell.com/manuals**.

Power Connection

Modular switches receive power from the Dell Blade Server chassis. For more information about the power supply for modular switches, see the *Dell Blade Server Chassis Hardware Owner's Manual,* which is located on the Dell Support website at **www.support.dell.com/manuals**.

Downloaded from www.Manualslib.com manuals search engine

4

Hardware Description

Overview

This section contains information about device characteristics and modular hardware configurations for the Dell™ PowerConnect™ M6220/M6348/M8024. The topics covered in this section include:

- PowerConnect Front Panel
- Console (RS-232) Port
- Physical Dimensions
- Power Supplies
- Ventilation System
- Stacking
- PowerConnect LED Definitions

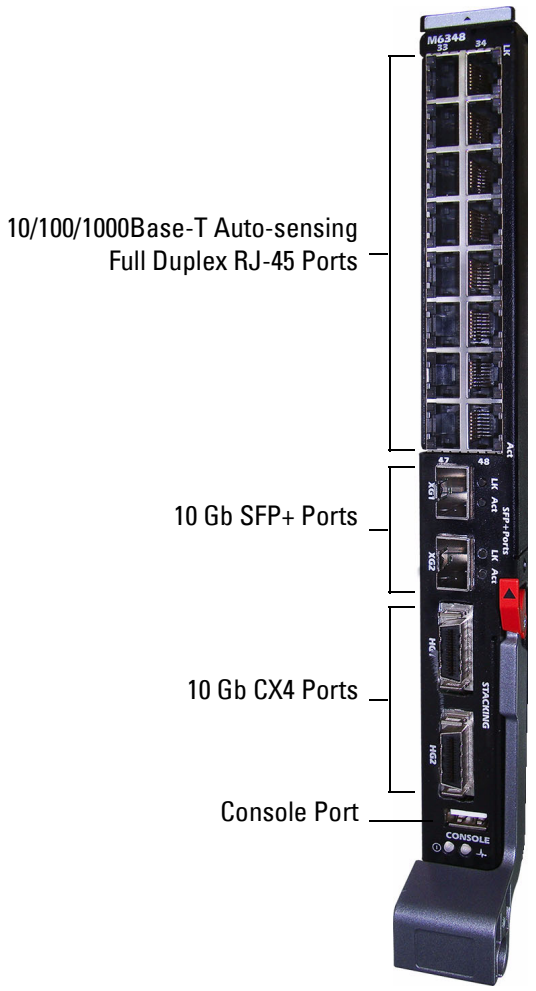
Downloaded from www.Manualslib.com manuals search engine

PowerConnect Front Panel

PowerConnect M6348 Front Panel

The PowerConnect M6348 front panel provides 16 10/100/1G Base-T ports. There are also 32 internal 1 gigabit ports that connect to each of the server blades.

Figure 4-1. PowerConnect M6348

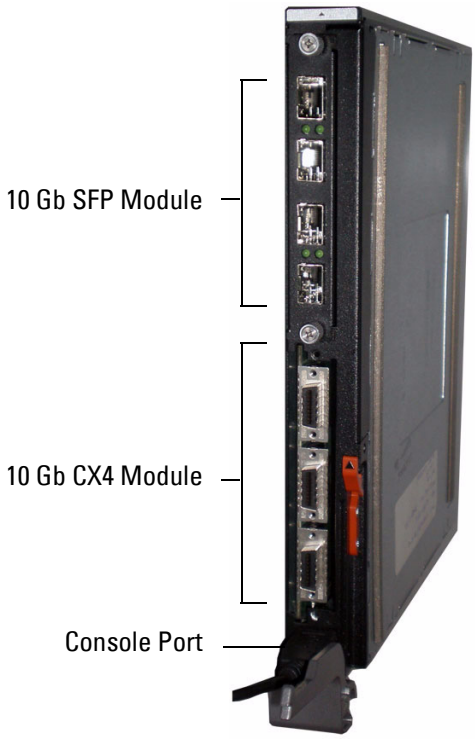


Downloaded from www.Manualslib.com manuals search engine

PowerConnect M8024 Front Panel

The PowerConnect M8024 front panel supports up to eight 10-gigabit ports. It has two 10-gigabit bays that can support SFP+, CX-4, or 10GBase-T modules. The SFP+ Module supports 4 ports, the CX-4 module supports 3 ports, and the 10GBase-T module supports 2 ports. The modules can be used in any combination and are sold separately. There are also 16 internal 10-gigabit ports that connect to each of the server blades.

Figure 4-2. PowerConnect M8024



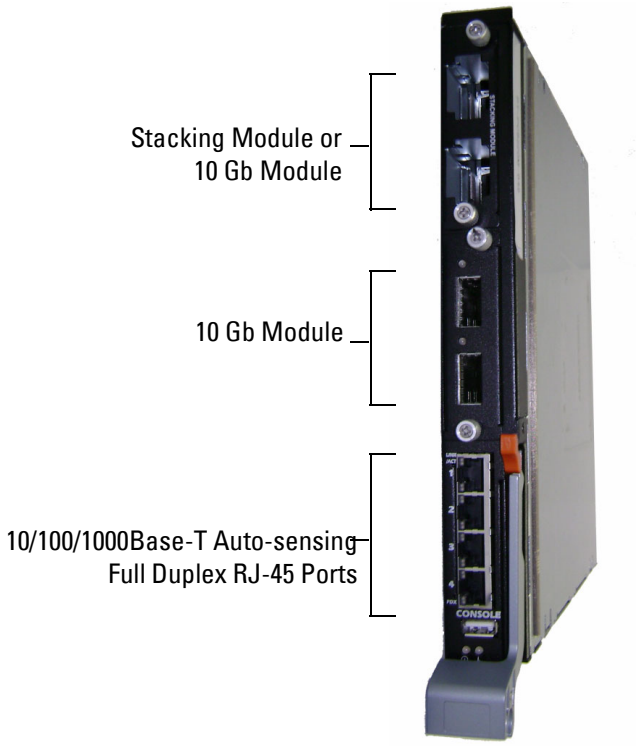
The 10GBase-T ports support 100-Megabit, 1-Gigabit, and 10-Gigabit Full Duplex speeds.

Downloaded from www.Manualslib.com manuals search engine

PowerConnect M6220 Front Panel

The PowerConnect M6220 front panel provides four 10/100/1000 Base-T RJ-45 ports. The front panel has two 10-gigabit bays that can support Stacking, CX-4, SFP+, XFP, or 10GBase-T modules. Each module provides support for 2 ports. The stacking module can only be used in Bay 1; the 10Gbase-T module can only be used in Bay 2. The modules are sold separately. There are also 16 internal ports that connect to each of the server blades.

Figure 4-3. PowerConnect M6220



- The switch automatically detects crossed and straight-through cables on RJ-45 ports.
- The 10/100/1000Base-T Auto-sensing RJ-45 ports support half- and full-duplex mode.

Downloaded from www.Manualslib.com manuals search engine

Console (RS-232) Port

The console (RS-232) port is used only for management through a serial interface. This port provides a direct connection to the switch and is used to access the CLI from a console terminal connected to an EIA/TIA-232 port.

To connect from the console port on the PowerConnect M6220/M6348/M8024 to a terminal, use the supplied serial cable with a USB Type A connector on one end and a female DB-9 connector on the other end. The console port on the PowerConnect M6220/M6348/M8024 is a USB port located on the bottom of the front panel.

Note: The console port supports asynchronous data of eight data bits, one stop bit, no parity bit, and no flow control. The default baud rate is 9600 bps.

Note: If you are installing a *stack* of switches, you need to assemble and cable the stack before powering up and configuring it. When a stack is powered up for the first time, the switches elect a Master Switch, which may occupy any location in the stack. Connect the terminal to the Master Switch. If you connect the terminal to a subordinate switch, you will not be able to use the CLI.

Console Redirect

The Dell M1000e Server Chassis includes a console redirect feature that allows you to manage each PowerConnect M6220/M6348/M8024 module from a single serial connection to the chassis. For more information about console redirect, see the *Dell Blade Server CMC User's Guide*.

Note: When you use console redirect to access a module, the external console port on that module is inactive and any current console sessions are terminated.

Physical Dimensions

For information about the PowerConnect M6220/M6348/M8024 physical dimensions, see the *Dell Blade Server Chassis Hardware Owner's Manual*, which is located on the Dell Support website at **www.support.dell.com**.

Power Supplies

For information about the PowerConnect M6220/M6348/M8024 power supplies, see the *Dell Blade Server Chassis Hardware Owner's Manual,* which is located on the Dell Support website at **www.support.dell.com**.

Ventilation System

For information about the PowerConnect M6220/M6348/M8024 ventilation system, see the *Dell Blade Server Chassis Hardware Owner's Manual,* which is located on the Dell Support website at **www.support.dell.com**.

Downloaded from www.Manualslib.com manuals search engine

Stacking

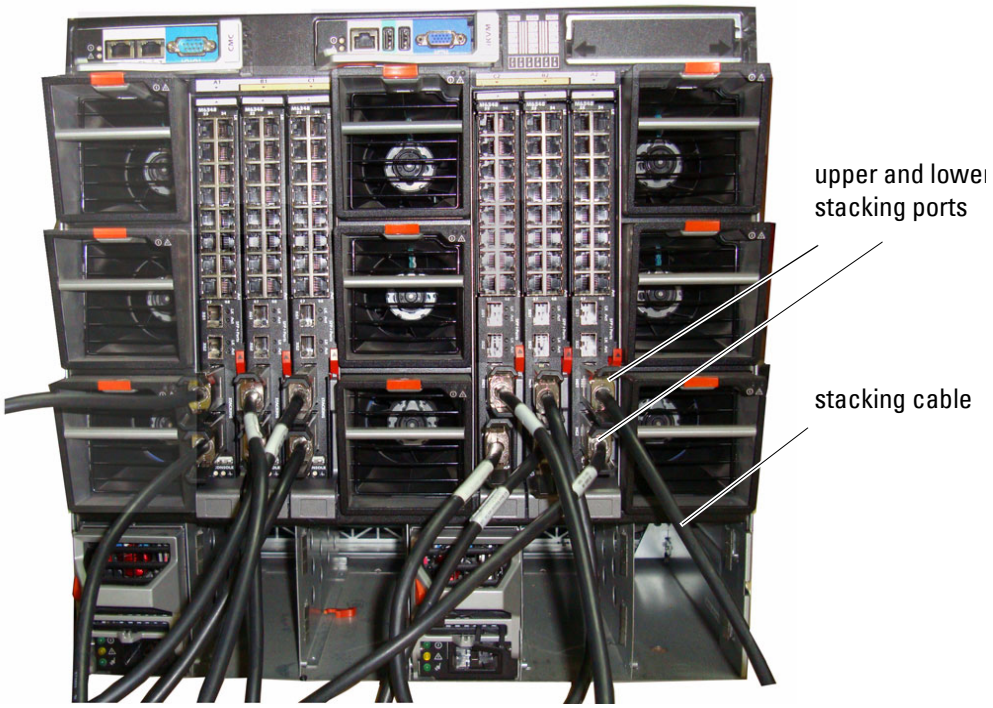
PowerConnect M6348 Stacking

You can stack up to 12 PowerConnect M6348, supporting up to 576 1-GB ports. Create a stack by connecting adjacent units using the stacking ports on the bottom of the switch panel. See Figure 4-5.

Note: The PowerConnect M6348 and M6220 can not be stacked together.

1. For each switch in the stack, connect one of the short stacking cables from stacking port one on the switch to stacking port two on the next switch.
2. If necessary, use a separately purchased, long (3 meter) stacking cable to connect the switches. Repeat this process until all of the devices are connected.
3. Use the remaining stacking cable to connect the remaining free ports, from port one of the last switch to port two of the first switch.

Figure 4-4. Connecting a Stack of PowerConnect M6348 Switches



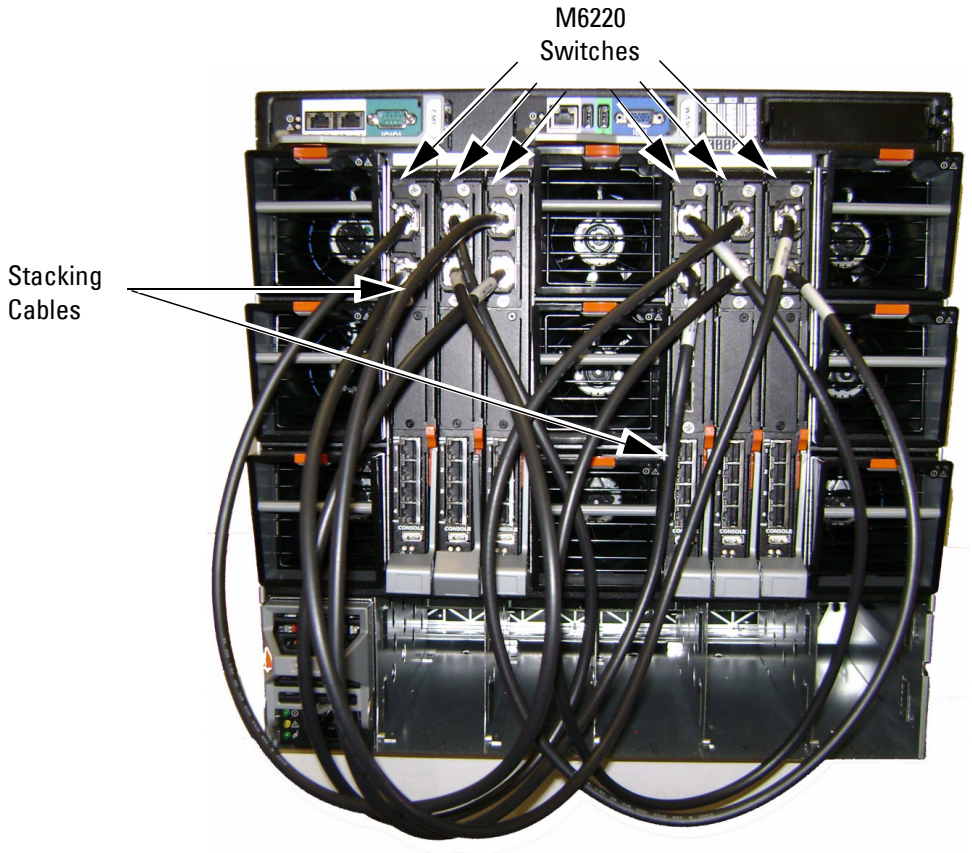
Downloaded from www.Manualslib.com manuals search engine

PowerConnect M6220 Stacking

You can stack up to 12 PowerConnect M6220 units, supporting up to 240 1-Gb ports. Create a stack by connecting adjacent units using the stacking ports on the top of the switch panel. See Figure 4-5.

1. Install a separately purchased stacking module in Bay 1 of each of the switches in the stack.
2. For each switch in the stack, connect one of the short stacking cables from stacking port one on the switch to stacking port two on the next switch.
3. If necessary, use a separately purchased, long (3 meter) stacking cable to connect the switches. Repeat this process until all of the devices are connected.
4. Use the remaining stacking cable to connect the remaining free ports, from port one of the last switch to port two of the first switch.

Figure 4-5. Connecting a Stack of PowerConnect M6220 Switches



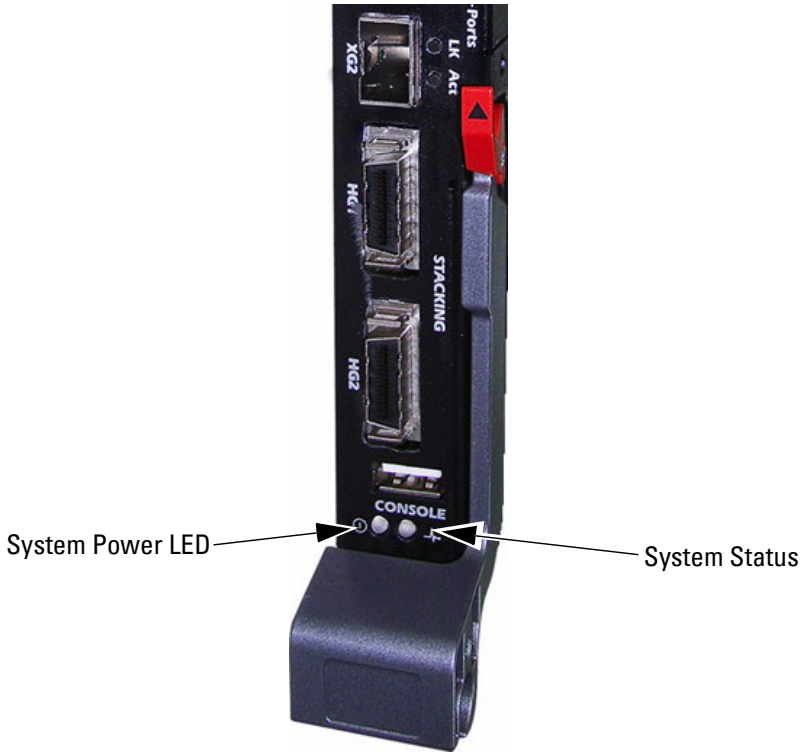
Downloaded from www.Manualslib.com manuals search engine

In Figure 4-4 and Figure 4-5, the stack has six M6220 switches connected through the stacking ports. The first stacking port on each switch is physically connected to the second stacking port on the next switch by using a stacking cable. The first stacking port on switch six is connected to the second stacking port on switch one.

PowerConnect LED Definitions

PowerConnect M6348 LEDs

Figure 4-6. PowerConnect M6348 LEDs



Downloaded from www.Manualslib.com manuals search engine

Table 4-1 contains the System Status LED definitions.

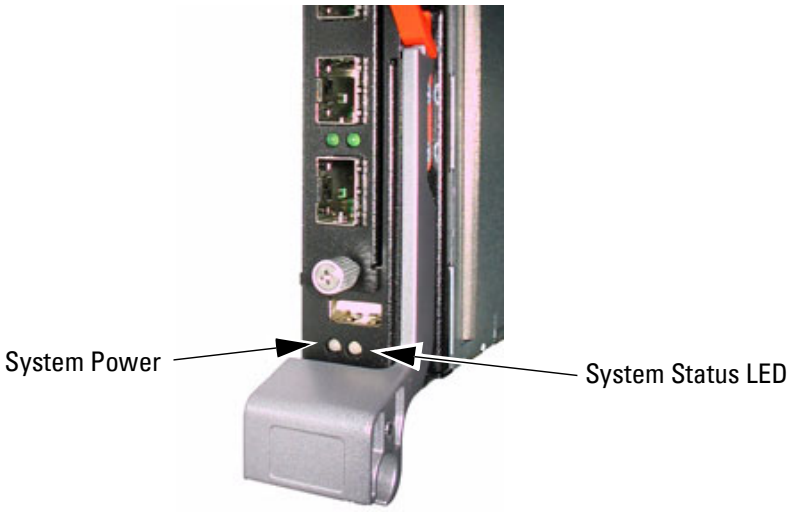
Table 4-1. PowerConnect M6348 Power and Status LED Definitions

LED	Color	Definition
	Green	Power is being supplied to the PowerConnect M6348 module
	Off	The PowerConnect M6348 does not have power.
	Blue	The switch is the stack master.
	Off	The switch is not the stack master.
	Amber	A fault has occurred, or the switch is booting.

PowerConnect M8024 LEDs

The front panel contains light emitting diodes (LEDs) that provide information about the status of the PowerConnect M8024 unit.

Figure 4-7. Front Panel LEDs



Downloaded from www.Manualslib.com manuals search engine

Table 4-2 contains the System Status LED definitions.

Table 4-2. PowerConnect M8024 Power and Status LED Definitions

LED	Color	Definition
	Green	Power is being supplied to the PowerConnect M8024 module
	Off	The PowerConnect M8024 does not have power.
	Blue	The switch is operating normally.
	Amber	A fault has occurred, or the switch is booting.

PowerConnect M6220 LEDs

The front panel contains light emitting diodes (LEDs) that indicate the status of links for the built-in 1Gb ports and the system status.

Figure 4-8. Front Panel LEDs

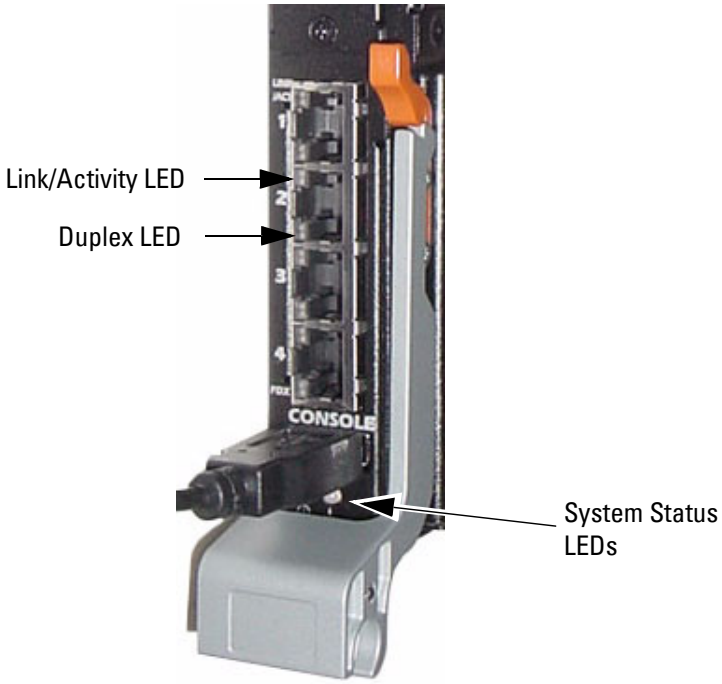


Table 4-3 contains the System Status LED definitions.

Downloaded from www.Manualslib.com manuals search engine

Table 4-3. M6220 Status LEDs Definitions

LED	Color	Definition
	Green	Power is being supplied to the M6220 module
	Off	The M6220 does not have power.
	Blue	The switch is the stack master.
	Off	The switch is not the stack master.
	Amber	A fault has occurred

SFP+ Port LEDs

Table 4-4 contains SFP+ port LED definitions for the PowerConnect M6220 and M8024.

Table 4-4. SFP+ Port LEDs Definitions

LED	Color	Definition
LNK/ACT	Solid Green	The port is linked.
	Flashing Green	The port is sending and/or receiving network traffic.
	Off	The port is not linked.

XFP Module Port LEDs

The XFP connectors are on the XFP module when it is inserted in the PowerConnect M6220. Table 4-5 contains XFP port LED definitions.

Table 4-5. XFP Port LEDs Definitions

LED	Color	Definition
XFP	Green	The port is linked.
	Flashing Green	The port is sending and/or receiving network traffic.
	Off	The port is not linked.

10/100/1000 Base-T Port LEDs

Each 10/100/1000 Base-T port has two LEDs. The following figure illustrates the 10/100/100 Base-T port LEDs.

Downloaded from www.Manualslib.com manuals search engine

Figure 4-9. 10/100/1000 Base-T Port LEDs

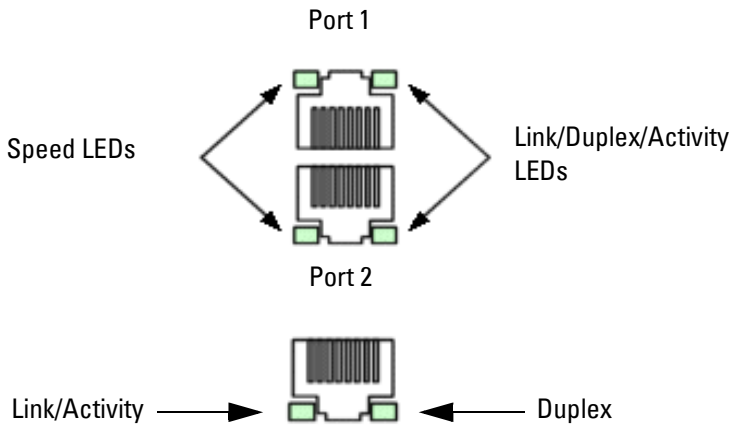


Table 4-6 contains 10/100/1000 Base-T port LED definitions.

Table 4-6. 10/100/1000 Base-T Port Definitions

LED	Color	Definition
Link/Activity	Green	The port is operating at 1000 Mbps.
	Amber	The port is operating at 10/100 Mbps.
	Solid	Link but no activity.
	Blinking	Link and activity.
	Off	No link.
Duplex	Green	Full duplex mode.
	Off	Half duplex mode.

10 Gb Base-T Module LEDs

Each 10 Gb Base-T Module has three LEDs.

Table 4-7 contains 10 Gb Base-T port LED definitions for the PowerConnect M6220 and M8024.

Table 4-7. 10 Gb Base-T Module Definitions

LED	Color	Definition
Link/Activity	Solid Green	The link is operating at 10 Gbps.
	Solid Yellow	The link is operating at other than 10 Gbps.

Downloaded from www.Manualslib.com manuals search engine

Table 4-7. 10 Gb Base-T Module Definitions

LED	Color	Definition
	Off	No link.
Act	Blinking Green	Activity.
	Off	No activity.
Wrong Bay	Solid Red	Module is in the wrong bay.

Note: On the PowerConnect M6220, the module must be inserted into Bay 2 to operate. When the module is inserted into Bay 1, it will not operate and the Wrong Bay LED is solid red.

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

5

Configuring Dell™ PowerConnect™

Overview

This chapter describes the initial switch configuration. Topics covered include:

- Starting the CLI
- General Configuration Information
- Booting the Switch
- Configuration Overview
- Advanced Configuration
- Software Download and Reboot
- Boot Menu Functions
- Sample Configuration Process

After completing all external connections, connect a terminal to the switch to monitor the boot process and other procedures.

Then, follow the order of installation and configuration procedures illustrated in Figure 5-1. For the initial configuration, perform the standard switch configuration. Performing other functions is described later in this section.

Note: Before proceeding, read the release notes for this product. You can download the release notes from the Dell Support website at **support.dell.com**.

Downloaded from www.Manualslib.com manuals search engine

Starting the CLI

To begin running the CLI, perform the following steps:

Note: The following steps are for use on the console line only.

1. Start the switch and wait until the startup procedure is complete. The **Easy Setup Wizard** welcome message now displays.

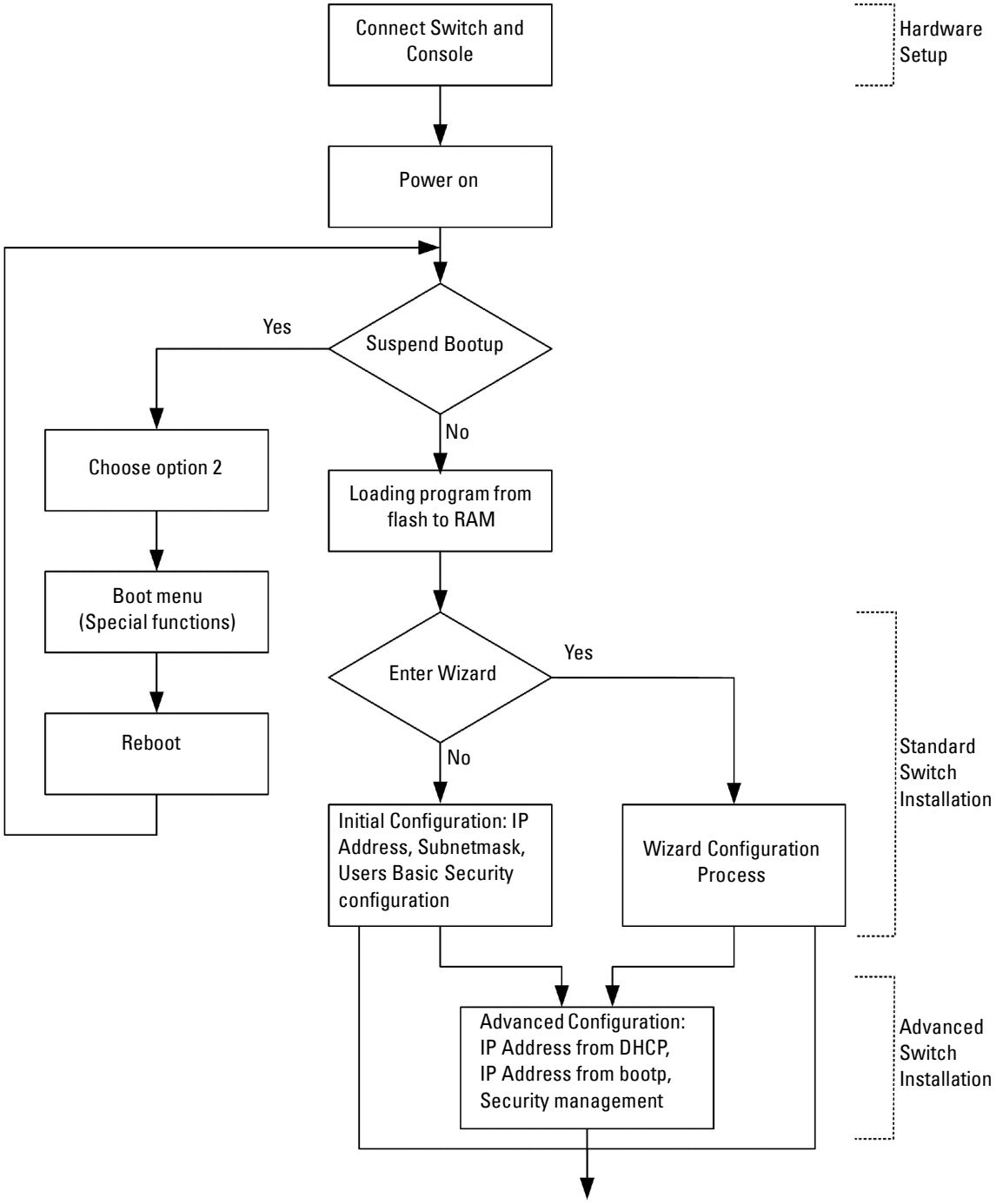
   Note: If you are using the autoconfig feature, do not use the Easy Setup Wizard.

2. Configure the switch using the **Easy Setup Wizard** and enter the necessary commands to complete the required tasks.
3. When finished, exit the session with the **quit** or **exit** command.

The switch can be managed over a direct connection to the switch console port, or through a Telnet connection. You can access the switch without a user account if you're directly connected to the switch. However, to access the switch through Telnet, at least one user account must be defined. Also, if access is through a Telnet connection, the switch must have a defined IP address, corresponding management access granted, and a workstation connected to the switch before using CLI commands.

Downloaded from www.Manualslib.com manuals search engine

Figure 5-1. Installation and Configuration Flow Chart



Downloaded from www.Manualslib.com manuals search engine

General Configuration Information

The PowerConnect M6220/M6348/M8024 switches are delivered with binary files containing the switch operating system and ASCII configuration files that are used to define the relationship of the switch to its network environment. The configuration process consists of adjusting the ASCII configuration files so that each switch fits into its unique network topology.

Terminal Connection Configuration

Your switch requires the following terminal connection parameters for configuration:

- no parity
- one stop bit
- 8 data bits
- no flow control

Baud Rate

The baud rates can be manually changed to any of the following values:

- 2400
- 4800
- 9600 (default baud rate)
- 19200
- 38400
- 57600
- 115200

The following is an example configuration for changing the default baud rate using CLI commands:

```
console#configure
console(config)#line console
console(config-line)#speed 115200
```

Note: Remember to set the baud rate on the terminal emulator software on your workstation to match the speed of the switch.

Other Configuration Requirements

The following is required for downloading embedded software and configuring the switch:

- ASCII terminal (or emulation) connected to the serial port (cross-cable) in the rear of the unit
- Assigned IP address for the switch for switch remote control use with Telnet, SSH, and so forth

Downloaded from www.Manualslib.com manuals search engine

Booting the Switch

When the power is turned on with the local terminal already connected, the switch goes through Power On Self Test (POST). POST runs every time the switch is initialized and checks hardware components to determine if the switch is fully operational before completely booting.

If a critical problem is detected, the program flow stops. If POST passes successfully, a valid executable image is loaded into RAM.

POST messages are displayed on the terminal and indicate test success or failure.

To boot the switch, perform the following steps:

1. Ensure that the serial cable is connected to the terminal.
2. Connect the power supply to the switch.
3. Turn on the switch.

   As the switch boots, the boot test first counts the switch memory availability and then continues to boot.
4. During boot, you can use the **Boot** menu, if necessary to run special procedures. To enter the **Boot** menu, press 2 within the first ten seconds after the following message appears.

   ```
   Select an option. If no selection in 10 seconds then
   operational code will start.

   1 - Start operational code.
   2 - Start Boot Menu.
   Select (1, 2):2
   ```

   For information about the **Boot** menu, see "Boot Menu Functions." The following text is an example of the entire displayed POST:

   ```
   CPU Card ID: 0x508548
   Mounting TFFS System ...
   Device details...

   volume descriptor ptr (pVolDesc):    0x1ae4898
   XBD device block I/O handle: 0x10001
   auto disk check on mount:      NOT ENABLED
   volume write mode:         copyback (DOS_WRITE)
   max # of simultaneously open files:    22
   ```


Downloaded from www.Manualslib.com manuals search engine

```
file descriptors in use:       0
# of different files in use:       0
# of descriptors for deleted files:    0
# of  obsolete descriptors:        0

current volume configuration:
 - volume label:    NO LABEL ; (in boot sector:              )
 - volume Id:       0x0
 - total number of sectors:   61,076
 - bytes per sector:     512
 - # of sectors per cluster: 4
 - # of reserved sectors:    1
 - FAT entry size:      FAT16
 - # of sectors per FAT copy:    60
 - # of FAT table copies:   2
 - # of hidden sectors:      4
 - first cluster is in sector #  136
 - Update last access date for open-read-close = FALSE
 - directory structure:         VFAT
 - file name format:            8-bit (extended-ASCII)
 - root dir start sector:               121
 - # of sectors per root:               15
 - max # of entries in root:            240

FAT handler information:
------------------------
 - allocation group size:       2 clusters
 - free space on volume:        20,733,952 bytes
```


Downloaded from www.Manualslib.com manuals search engine

```
Boot Menu May 25 2009
Select an option. If no selection in 10 seconds then
operational code will start.

1 - Start operational code.
2 - Start Boot Menu.
Select (1, 2):2

Boot Menu Version: 31 October 2007

Options available
1  - Start operational code
2  - Change baud rate
3  - Retrieve event log using XMODEM
4  - Load new operational code using XMODEM
5  - Display operational code vital product data
7  - Update boot code
8  - Delete backup image
9  - Reset the system
10 - Restore configuration to factory defaults (delete config files)
11 - Activate Backup Image
12 - Password Recovery Procedure
[Boot Menu]
```

The boot process runs approximately 60 seconds.

The auto-boot message that appears at the end of POST (see the last lines) indicates that no problems were encountered during boot. To return to operational code from the [Boot Menu] prompt, press 1.

The following output displays an example configuration. Items such as addresses, versions, and dates may differ for each switch.

```
Operational Code Date: Tue May 26 14:12:20 2009
Uncompressing.....
```


Downloaded from www.Manualslib.com manuals search engine

```
Target Name: vxTarget
Attached IPv4 interface to motetsec unit 0

Adding 70447 symbols for standalone.
 CPU: Broadcom SBC8548.  Processor #0.
 Memory Size: 0x20000000.  BSP version 2.0/2.
 Created: May 26 2009, 13:11:31
 ED&R Policy Mode: deployed
 WDB Comm Type: WDB_COMM_END
 WDB: Ready.
remLib: Not initialized.
remLib: Not initialized.
CFI Probe: Found 2x16 devices in x16 mode

volume descriptor ptr (pVolDesc):    0x706d770
XBD device block I/O handle: 0x10001
auto disk check on mount:      NOT ENABLED
volume write mode:         copyback (DOS_WRITE)
max # of simultaneously open files:    52
file descriptors in use:       0
# of different files in use:       0
# of descriptors for deleted files:    0
# of  obsolete descriptors:        0

current volume configuration:
 - volume label:    NO LABEL ; (in boot sector:              )
 - volume Id:       0x0
 - total number of sectors:   124,408
```


Downloaded from www.Manualslib.com manuals search engine

```
 - bytes per sector:     512
 - # of sectors per cluster: 4
 - # of reserved sectors:    1
 - FAT entry size:      FAT16
 - # of sectors per FAT copy:    122
 - # of FAT table copies:   2
 - # of hidden sectors:      8
 - first cluster is in sector #  260
 - Update last access date for open-read-close = FALSE
 - directory structure:         VFAT
 - file name format:            8-bit (extended-ASCII)
 - root dir start sector:               245
 - # of sectors per root:               15
 - max # of entries in root:            240

FAT handler information:
------------------------
 - allocation group size:       4 clusters
 - free space on volume:        44,380,160 bytes


PCI unit 0: Dev 0xb624, Rev 0x12, Chip BCM56624_B1, Driver BCM56624_B0
SOC unit 0 attached to PCI device BCM56624_B1
Adding BCM transport pointers
Configuring CPUTRANS TX
Configuring CPUTRANS RX
st_state(0) = 0x0
st_state(1) = 0x2
```


Downloaded from www.Manualslib.com manuals search engine

```
<186> JAN 01 00:00:15 0.0.0.0-1 UNKN[536870176]: bootos.c(218) 1 %
Event(0xaaaaaaaa)

Instantiating RamCP: as rawFs,  device = 0x20001

Formatting RamCP: for DOSFS

Instantiating RamCP: as rawFs, device = 0x20001

Formatting...OK.


(Unit 1 - Waiting to select management unit)>


Applying Global configuration, please wait ...


Applying Interface configuration, please wait ...



console>
```

After the switch boots successfully, a prompt appears and you can use the local terminal to begin configuring the switch. However, before configuring the switch, ensure that the software version installed on the switch is the latest version. If it is not the latest version, download and install the latest version. See "Software Download and Reboot."

Downloaded from www.Manualslib.com manuals search engine

Configuration Overview

Before configuring the switch, obtain the following information from the network administrator:

- Is the network setup for the autoconfig feature?

  If the network is setup for autoconfig, manual configuration of the switch is not necessary (skip the procedures in this section).
- IP subnet mask for the network
- Default gateway (next hop router) IP address for configuring the default route

There are two types of configuration:

- *Initial* configuration consists of configuration functions with basic security considerations.
- *Advanced* configuration includes dynamic IP configuration and more advanced security considerations.

Note: After making any configuration changes, the new configuration must be saved before rebooting. To save the configuration, enter:

```
console#copy running-config startup-config
```

Easy Setup Wizard

An **Easy Setup Wizard** displays when the system boots up without a configuration or with only the default factory configuration. The **Easy Setup Wizard** is designed to guide you through some initial steps to set up basic system configuration and security and to make the switch manageable. The **Easy Setup Wizard** requires that the initial administrator account be setup when turning up the switch. This administrative account setup by the wizard has the highest privilege level (level 15).

The **Easy Setup Wizard** guides you in the basic initial configuration of a newly installed switch so that it can be immediately deployed, functional, and completely manageable through the Web, CLI, and the remote Dell Network Manager. After the initial set up, you may enter the system to set up more advanced configuration.

The system is setup with default management VLAN ID=1. The initial turn-up must be done through the serial interface.

The wizard sets up the following configuration on the switch:

- Establishes the initial privileged user account with a valid password. The wizard configures one privileged user account during the set up. The initial account is given the highest privilege level (level 15).
- Enables CLI login and HTTP/HTTPS access to use the local authentication setting only. You may return later to configure Radius or TACACS+.
- Sets up the IP address for the management VLAN.

Downloaded from www.Manualslib.com manuals search engine

- Sets up the SNMP community string to be used by the SNMP manager at a given IP address. You may choose to skip this step if SNMP management is not used for this switch. If it is configured, the default access level is set to the highest available access for the SNMP management interface. Initially only SNMPv1/2c is activated. SNMPv3 is disabled until you return to configure security access for SNMPv3 (for example, engine ID, view, etc.). The SNMP community string may include spaces. The wizard requires the use of quotation marks when you want to enter spaces in the community string. Although spaces are allowed in the community string, their use is discouraged. The default community string contains no spaces.
- Allows you to specify the management server IP or permit SNMP access from all IP addresses.
- Sets up the default gateway IP address.
- Allows simple mode to be set.

If you do not use the wizard initially, the session defaults to the CLI mode. The set-up wizard continues to display each time you login until a configuration is saved. Once saved, the wizard option is only presented again if you reset the switch to the factory-default settings.

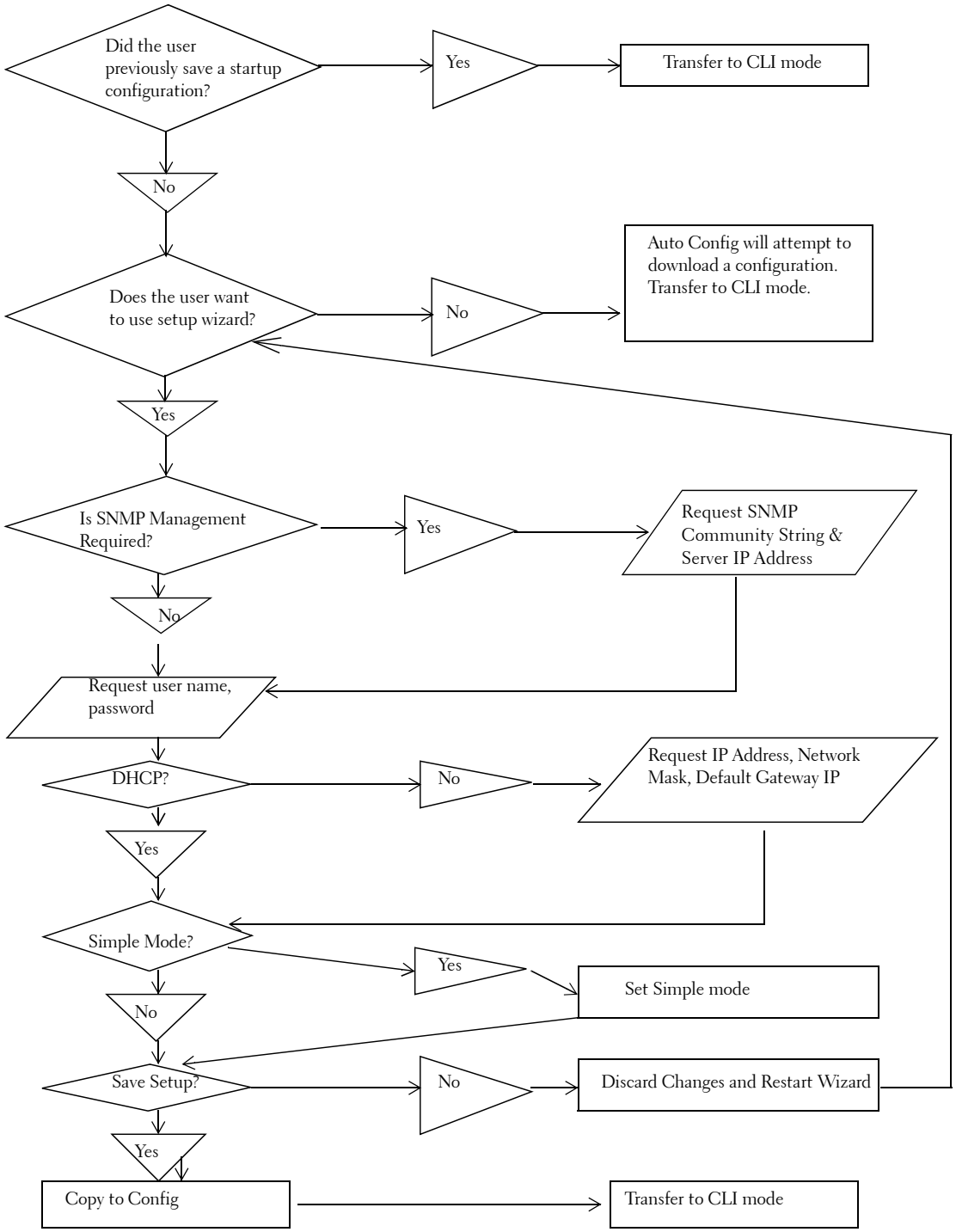
Since a switch may be powered on in the field without a serial connection, the switch waits 60 seconds for you to respond to a set-up prompt if the switch has not yet been configured. If there is no response, the switch continues normal operation using the default factory configuration. The next time the system reboots you are given another opportunity to run the set-up wizard.

Functional Flow

The following functional flow diagram illustrates the procedures for the **Easy Setup Wizard**.

Downloaded from www.Manualslib.com manuals search engine

Figure 5-2. Setup Wizard Flow Chart



Downloaded from www.Manualslib.com manuals search engine

Example of an Easy Setup Wizard Session

This section describes an **Easy Setup Wizard** session. See the state diagram (Figure 5-2) for the general flow. The values used by the following session are examples only. Please request the actual values from your network adminstrator(s):

- IP address for the management VLAN is 192.168.1.1:255.255.255.0.
- The user name is *admin*, and password is *admin123*.
- The network management system IP address is 192.168.1.10.
- The default gateway is 192.168.1.100.
- The SNMP community string to be used is *Dell_Network_Manager*.

The setup wizard configures the initial values as defined above. After you complete the wizard, the system is configured as follows:

- SNMPv1/2c is enabled and the community string is set up as defined above. SNMPv3 is disabled.
- The admin user account is set up as defined.
- A network management system is configured. From this management station, you can access the SNMP, HTTP, and CLI interfaces. You may also choose to allow all IP addresses to access these management interfaces by choosing the (0.0.0.0) IP address.
- An IP address is configured for the default management VLAN (1).
- A default gateway address is configured.

Note: In the example below, the possible user options are enclosed in [ ]. Also, where possible, the default value is provided in { }. If you enter <Return> with no options defined, the default value is accepted. Help text is in parentheses.

The following example contains the sequence of prompts and responses associated with running an example Dell **Easy Setup Wizard** session, using the input values listed above.

```
Unit 1 - Waiting to select management unit)>

Applying Global configuration, please wait ...

Welcome to Dell Easy Setup Wizard

The Setup Wizard guides you through the initial switch configuration, and
gets you up and running as quickly as possible. You can skip the setup
wizard, and enter CLI mode to manually configure the switch. You must
respond to the next question to run the setup wizard within 60 seconds,
otherwise the system will continue with normal operation using the
default system configuration.Note: You can exit the setup wizard at any
point by entering [ctrl+z].

Would you like to run the setup wizard (you must answer this question
within 60 seconds)? [Y/N] y

Step 1:
```


Downloaded from www.Manualslib.com manuals search engine

The system is not setup for SNMP management by default. To manage the switch using SNMP (required for Dell Network Manager) you can

. Set up the initial SNMP version 2 account now.

. Return later and setup other SNMP accounts. (For more information on setting up an SNMP version 1 or 3 account, see the user documentation).

Would you like to setup the SNMP management interface now? [Y/N] n

Step 2:

Now we need to setup your initial privilege (Level 15) user account. This account is used to login to the CLI and Web interface. You may setup other accounts and change privilege levels later. For more information on setting up user accounts and changing privilege levels, see the user documentation.

To setup a user account:

Please enter the user name. [root]:root

Please enter the user password:

Please reenter the user password:

Step 3:

Next, an IP address is setup. The IP address is defined on the default VLAN (VLAN #1), of which all ports are members. This is the IP address you use to access the CLI, Web interface, or SNMP interface for the switch. Optionally you may request that the system automatically retrieve an IP address from the network via DHCP (this requires that you have a DHCP server running on the network).

To setup an IP address:

Please enter the IP address of the device (A.B.C.D) or enter "DHCP" (without the quotes) to automatically request an IP address from the network DHCP server. [192.168.2.1]:

Please enter the IP subnet mask (A.B.C.D or /nn). [255.255.255.0]:

Step 4:

Finally, setup the default gateway. Please enter the IP address of the gateway from which this network is reachable. [0.0.0.0]:

This is the configuration information that has been collected:

User Account setup = root

Password = ********

Downloaded from www.Manualslib.com manuals search engine

```
Management IP address = 192.168.2.1 255.255.255.0

Default Gateway = 0.0.0.0

Operation Mode = Normal

Step 5:

Do you want to select the operational mode as Simple Mode? [Y/N] n

Final Step:

If the information is correct, please select (Y) to save the
configuration, and copy to the start-up configuration file. If the
information is incorrect, select (N) to discard configuration and
restart the wizard: [Y/N] y

Thank you for using Dell Easy Set up Wizard. You will now enter CLI mode.

Applying Interface configuration, please wait...

console>
```

Advanced Configuration

CLI Basics

The `help` command in the User EXEC mode and privileged EXEC mode displays the keyboard short cuts. Following is the sample display of the help command:

```
Console>help


HELP:

Special keys:

  DEL, BS .... delete previous character

  Ctrl-A  .... go to beginning of line

  Ctrl-E  .... go to end of line

  Ctrl-F  .... go forward one character

  Ctrl-B  .... go backward one character

  Ctrl-D  .... delete current character

  Ctrl-U, X .. delete to beginning of line
```


Downloaded from www.Manualslib.com manuals search engine

```
Ctrl-K  .... delete to end of line
Ctrl-W  .... delete previous word
Ctrl-T  .... transpose previous character
Ctrl-P  .... go to previous line in history buffer
Ctrl-R  .... rewrites or pastes the line
Ctrl-N  .... go to next line in history buffer
Ctrl-Y  .... print last deleted character
Ctrl-Z  .... return to root command prompt
Ctrl-Q  .... enables serial flow
Ctrl-S  .... disables serial flow
Tab, <SPACE> command-line completion
Exit    .... go to next lower command prompt
?       .... list choices
```

Context Sensitive Help

Use the **?** command to get context sensitive help in the CLI. It can be used to get the list of possible sub-commands or to list possible commands starting with some partially entered commands. The **?** command when specified on an empty line provides the list of commands possible for the given level in the command tree. The **?** can also be used within a command input to return the list of parameters that are required to fully complete the command. Parameters that are already provided by the user is left out of the command list so that only the missing parameters are listed.

Interface Naming Convention

In an industry-standard CLI implementation, there is an accepted convention for naming interfaces on the CLI. The convention for naming interfaces on Dell devices are as follows:

- **Unit#/Interface ID** — each interface is identified by the *Unit#* followed by a /symbol and then the *Interface ID* (see below). For example, **2/g10** identifies gigabit port 10 within the second unit of a stack.
- **Unit#** — the unit number is used only in a stacking solution where a number of switches are stacked to form a virtual device. In this case, the *unit number* identifies the physical device identifier within the stack.
- **Interface ID** — is formed by the interface type followed by the interface number. There is currently a predefined list of *interface types* (see below). If additional interface types are to be defined, they must be registered with Dell. For example, **1/xg10** identifies the 10-gigabit port 10 on the first unit.

Downloaded from www.Manualslib.com manuals search engine

- **Interface Types** — the following interface types are defined in the PowerConnect M6220/M6348/M8024 switches:
  - **xg** — 10 Gb Ethernet port (for example, 1/**xg2** is the 10 Gb Ethernet port 2).

M6220, M6348, and M8024CLI Reference Guide

For detailed information on all the CLI commands available, see the *CLI Reference Guide.*

This section provides summary information about such common tasks as:

- Modifying Switching Port Default Settings
- Retrieving an IP Address From a DHCP Server
- Configuring an Initial Console Password
- Configuring an Initial Telnet Password
- Configuring an Initial HTTP Password
- Configuring an Initial HTTPS Password

Downloaded from www.Manualslib.com manuals search engine

Modifying Switching Port Default Settings

When configuring/receiving IP addresses through DHCP and BOOTP, the configuration received from these servers includes the IP address, and may include subnet mask and default gateway.

When you first log in, the CLI enters the root of the command hierarchy. To go to a different level of the command hierarchy, enter commands such as **configure**, which causes the CLI to enter the *config* sub tree. To go back to the previous level in the command hierarchy, use the exit command.

```
SwitchA#configure
SwitchA(config)#exit
SwitchA#
```

The following examples show the system prompts used by the PowerConnect M6220/M6348/M8024 switches:

- **SwitchA>** — indicates that the device name is *SwitchA* and the CLI is current in the top level of the command hierarchy. The CLI is also in the *User EXEC mode*.
- **SwitchA#** — this prompt is similar to the above prompt except that the # indicates that the CLI is in a privilege EXEC mode (not in the User EXEC mode).
- **SwitchA(config)#** — indicates that the CLI is currently in the *global configuration* mode of the command hierarchy. Enter this mode by typing **configure** at the top level.
- **SwitchA(config-if)#** — this prompt indicates that the CLI is currently in the *interface* configuration mode. Enter this by typing **interface range ethernet**, **interface range port-channel**, or **interface range vlan** from the config mode. In this case, there is no specific reference to an interface so the system is operating on a generic set of interfaces.
- **SwitchA(config-if-1/xg1)#** — indicates that the CLI is currently operating on the 10 gigabit Ethernet interface 1.

Switching Port Default Settings

The following table describes the switch port default settings.

Table 5-1. Port Default Settings

Function	Default Setting
Port speed and mode	1G Auto-negotiation
Port forwarding state	Enabled
Head of line blocking prevention	On (Enabled)
Flow Control	On
Back Pressure	Off

Downloaded from www.Manualslib.com manuals search engine

The following is an example for changing the port description on port 1/g1 using CLI commands:

```
console(config)#interface ethernet 1/g1
console(config-if-1/g1)#description 100
```

Retrieving an IP Address From a DHCP Server

When using the DHCP protocol to retrieve an IP address, the switch acts as a DHCP client.

The out-of-band interface is configured by default to use DHCP. If the configuration has been changed, follow these steps to use DHCP:

1. Select and connect any port to a DHCP server or to a subnet that has a DHCP server on it, in order to retrieve the IP address.

   Note: You do not need to delete the switch configuration to retrieve an IP address for the DHCP server.

2. Enter the following commands to use the selected port for receiving the IP address.

   - Assigning Dynamic IP Addresses:

   ```
   console(config)#interface out-of-band
   console(config-if)#ip address dhcp
   ```

   The interface receives the IP address automatically.

3. To verify the IP address, enter the show ip interface out-of-band command at the system prompt as shown in the following example.

   ```
   console#show ip interface out-of-band


   IP Address..................................... 10.27.22.168
   Subnet Mask.................................... 255.255.255.0
   Default Gateway................................ 10.27.22.1
   ServPort Configured Protocol Current........... DHCP
   Burned In MAC Address......................... 0063.4802.0011


   console#
   ```


Downloaded from www.Manualslib.com manuals search engine

Security Management and Password Configuration

System security is handled through the AAA (Authentication, Authorization, and Accounting) mechanism that manages user access rights, privileges, and management methods. AAA uses both local and remote user databases. Data encryption is handled through the SSH mechanism.

The system is delivered with no default password configured; all passwords are user-defined. If a user-defined password is lost, a password recovery procedure can be invoked from the **Boot** menu. The procedure is applicable for the local terminal only and allows a one-time access to the switch from the local terminal with no password entered.

Configuring Security Passwords

The security passwords can be configured for the following services:

- Console
- Telnet
- SSH
- HTTP
- HTTPS

Note: When creating a user name, the default priority is "1," which allows access but not configuration rights. A priority of "15" must be set to enable access and configuration rights to the switch.

Configuring an Initial Console Password

To configure an initial console password, enter the following commands:

```
console(config)#aaa authentication login default line
console(config)#aaa authentication enable default line
console(config)#line console
console(config-line)#login authentication default
console(config-line)#enable authentication default
console(config-line)#password secret123
```

- When initially logging on to a switch through a console session, enter **secret123** at the password prompt.
- When changing a switch's mode to enable, enter **secret123** at the password prompt.

Downloaded from www.Manualslib.com manuals search engine

Configuring an Initial Telnet Password

To configure an initial Telnet password, enter the following commands:

```
console(config)#aaa authentication login default line
console(config)#aaa authentication enable default line
console(config)#line telnet
console(config-line)#login authentication default
console(config-line)#enable authentication default
console(config-line)#password pass1234
```

- When initially logging onto a switch through a Telnet session, enter **pass1234** at the password prompt.
- When changing a switch mode to enable, enter **pass1234**.

Configuring an Initial HTTP Password

To configure an initial HTTP password, enter the following commands:

```
console(config)#ip http authentication local
console(config)#username admin password user1234 level 15
```

Configuring an Initial HTTPS Password

To configure an initial HTTPS password, enter the following commands:

```
console(config)#ip https authentication local
```

Note: You should generate a new crypto certificate each time you upgrade (install a new version of) the control software application on the switch.

Enter the following commands once when configuring to use an HTTPS session over a console, a Telnet, or an SSH session.

Note: In the Web browser enable SSL 2.0 or greater for the page content to appear.

```
console(config)#crypto certificate 1 generate
console(config)#ip https server
```

Note: Http and Https services require level 15 access and connect directly to the configuration level access.

Downloaded from www.Manualslib.com manuals search engine

Software Download and Reboot

Software Download Through TFTP Server

This section contains instructions for downloading switch software (system and boot images) through a TFTP server. The TFTP server must be available on the network before downloading the software.

The switch boots and runs when decompressing the system image from the flash memory area where a copy of the system image is stored.

Notice: You must run the **boot system** command to activate the newly downloaded image.

On the next boot, the switch decompresses and runs the currently active system image unless chosen otherwise.

To download an image through the TFTP server:

1. Ensure that an IP address is configured on the out-of-band interface and pings can be sent to a TFTP server.
2. Ensure that the file to be downloaded is saved on the TFTP server (the **.stk** file).
3. Enter the command **show version** to verify which software version is currently running on the switch.

   The following is an example of the information that appears:

   ```
   console>show version

   Image Descriptions

    image1 : default image

    image2 :

   Images currently available on Flash

   ---------------------------------------------------------------
   unit image1 image2 current-activenext-active
   ---------------------------------------------------------------
   1    3.1.0.4 3.1.0.4 image1 image1
   ```

4. Enter the command **copy tftp://{*tftp address*}/{*file name*} image** to copy a new system image to the switch.

   When the new image is downloaded, it is saved in the area allocated for the other copy of system image (image2, as given in the example). The following is an example of the information that appears:

   ```
   console#copy tftp://10.254.24.64/pc62xxr0v34.stk image

   Mode............................................. TFTP

   Set TFTP Server IP............................... 10.254.24.64

   TFTP Path....................................... ./
   ```


Downloaded from www.Manualslib.com manuals search engine

```
TFTP Filename.................................. PC8024v3.1.0.x.stk
Data Type...................................... Code
Destination Filename........................... image

Management access will be blocked for the duration of the transfer
Are you sure you want to start? (y/n) y
```

5. Select the image for the next boot by entering the **boot system** command. After this command, enter the command **show version** to verify that the copy indicated as a parameter in the **boot system** command is selected for the next boot.

   The following is an example of the information that appears:

```
console#boot system image2
Activating image image2 ..
console>show version
Image Descriptions
 image1 : default image
 image2 :
Images currently available on Flash
---------------------------------------------------------------
unit image1 image2 current-activenext-active
---------------------------------------------------------------
1    3.1.0.0 3.1.0.1 image1 image2
```

   If the image for the next boot is not selected by entering the **boot system** command, the system boots from the currently active image (image1, as given in the example).

6. Enter the command **reload**. The following message displays:

```
console#reload
Management switch has unsaved changes.
Are you sure you want to continue? (y/n)
```

7. Enter y. The following message then displays.

```
Configuration Not Saved!
Are you sure you want to reload the stack? (y/n)
```

8. Enter y to reboot the switch.

Downloaded from www.Manualslib.com manuals search engine

Update Bootcode

Use the **update bootcode** command to update the bootcode on all switches. For each switch, the bootcode is extracted from the next-active image and programmed to flash. To update the bootcode for one switch, specify the unit in the command (as shown in the following example).

To show the boot code that's on a switch, reboot that switch. Build dates show during the boot process.

1. Enter the following command:

   ```
   console# update bootcode
   Updating boot code ...
   Boot code update completed successfully.
   ```

2. Enter the command **reload**.

   ```
   console#reload
   Are you sure you want to reload the stack? (y/n)
   ```

3. Enter **y** to reboot the switch.

Boot Menu Functions

You can perform many configuration tasks through the **Boot** menu, which can be invoked after the first part of the POST is completed.

To display the **Boot** menu:

1. During the boot process, press **2** within ten seconds after the following message displays:

   ```
   Boot Menu Version: 31 October 2007
   Select an option. If no selection in 10 seconds then
   operational code will start.

   1 - Start operational code.
   2 - Start Boot Menu.
   Select (1, 2):
   ```

   The **Boot** menu displays and contains the following configuration functions:

   ```
   1  - Start operational code
   2  - Change baud rate
   3  - Retrieve event log using XMODEM
   4  - Load new operational code using XMODEM
   ```


Downloaded from www.Manualslib.com manuals search engine

```
5  - Display operational code vital product data
7  - Update boot code
8  - Delete backup image
9  - Reset the system
10 - Restore configuration to factory defaults (delete config files)
11 - Activate Backup Image
12 - Password Recovery Procedure
```

The following sections describe the **Boot** menu options.

Start Operational Code

Use option 1 to resume loading the operational code.

To relaunch the boot process from the **Boot** menu:

1. On the **Boot** menu, select **1** and press <Enter>.

   The following prompt displays:

```
Operational Code Date: Tue Apr 29 10:15:36 2008
Uncompressing.....
                        50%                     100%
|||||||||||||||||||||||||||||||||||||||||||||||||||
```

Change the Baud Rate

Use option **2** to change the baud rate of the serial interface.

To change the baud rate from the **Boot** menu:

1. On the **Boot** menu, select **2** and press <Enter>.

   The following prompt displays:

```
[Boot Menu]2
Select baud rate:
1 - 1200
2 - 2400
3 - 4800
4 - 9600
5 - 19200
```


Downloaded from www.Manualslib.com manuals search engine

```
6 - 38400
7 - 57600
8 - 115200
0 - no change
```

Note: The selected baud rate takes effect immediately.

2. The boot process resumes.

Retrieve Event Log using XMODEM

Use option 3 to retrieve the event log and download it to your ASCII terminal.

To retrieve the event log from the **Boot** menu:

1. On the **Boot** menu, select **3** and press <Enter>.

   The following prompt displays:

```
[Boot Menu] 3
Sending event log, start XMODEM receive.....
File asciilog.bin Ready to SEND in binary mode
Estimated File Size 169K, 1345 Sectors, 172032 Bytes
Estimated transmission time 3 minutes 20 seconds
Send several Control-X characters to cancel before transfer starts.
```

2. The boot process resumes.

Load New Operational Code Using XMODEM

Use option 4 when a new software version must be downloaded to replace corrupted files, update, or upgrade the system software.

To download software from the **Boot** menu:

1. On the **Boot** menu, select **4** and press <Enter>.

   The following prompt displays:

```
[Boot Menu] 4
Ready to receive the file with XMODEM/CRC....
Ready to RECEIVE File xcode.bin in binary mode
Send several Control-X characters to cancel before transfer starts.
```

2. When using HyperTerminal, click **Transfer** on the **HyperTerminal** menu bar.
3. From the **Transfer** menu, click **Send File**.

Downloaded from www.Manualslib.com manuals search engine

The **Send File** window displays.

4. Enter the file path for the file to be downloaded.
5. Ensure the protocol is defined as Xmodem.
6. Click **Send**.

   The software is downloaded. Software downloading takes several minutes. The terminal emulation application, such as HyperTerminal, may display the loading process progress.

Display Operational Code Vital Product Data

Use option 5 to view boot image information.

To display boot image information from the **Boot** menu:

1. On the **Boot** menu, select **5** and press <Enter>.

   The following prompt displays:

```
[Boot Menu] 5

The following image is in the Flash File System:

File Name.....................................image1

CRC...........................................0xb017 (45079)

Target Device................................0x00508541

Size..........................................0x8ec50c (9356556)

Number of Components..........................2

Operational Code Size.........................0x7ec048 (8306760)

Operational Code Offset.......................0x74 (116)

Operational Code FLASH flag...................1

Operational Code CRC..........................0x9B4D

Boot Code Version.............................1

Boot Code Size................................0x100000 (1048576)

Boot Code Offset..............................0x7ec0bc (8306876)

Boot Code FLASH flag..........................0

Boot Code CRC.................................0x1CB8

VPD - rel 0 ver 31 maint_lvl 0

      Timestamp - Thu Jun  8 12:51:44 2006

      File - pc62xxr0v31.stk
```


Downloaded from www.Manualslib.com manuals search engine

2. The boot process resumes.

Update Boot Code

Use option 7 to update the boot code in the FLASH memory. This option is only valid after loading new boot code using Boot Menu option 4. User action is confirmed with a Y/N question before executing the command.

To download software from the **Boot** menu:

1. On the **Boot** menu, select **7** and press <Enter>.

   The following prompt displays:

   ```
   Do you wish to update Boot Code? (y/n) y
   Erasing Boot Flash.....Done.
   Wrote 0x10000 bytes.
   Wrote 0x20000 bytes.
   Wrote 0x30000 bytes.
   Wrote 0x40000 bytes.
   Wrote 0x50000 bytes.
   Wrote 0x60000 bytes.
   Boot code updated
   ```

2. The boot process resumes.

Delete Backup Image

Use option 8 to delete the backup image from the FLASH memory. User action is confirmed with a Y/N question before executing the command.

To delete the backup image from the **Boot** menu:

1. On the **Boot** menu, select **8** and press <Enter>.

   The following prompt displays:

   ```
   Are you SURE you want to delete backup image : image2 ? (y/n):y
   Backup image deleted...
   [Boot Menu]
   ```

2. The boot process resumes.

Downloaded from www.Manualslib.com manuals search engine

Reset the System

Use option 9 to clear all FLASH and reset the system to its default setting. User action is confirmed with a Y/N question before executing the command.

To reset the system from the **Boot** menu:

1. On the **Boot** menu, select **9** and press <Enter>.

   The following prompt displays:

   ```
   [Boot Menu] 9
   ```

   ```
   Are you SURE you want to reset the system? (y/n):y
   ```

2. The boot process starts over.

Restore Configuration to Factory Defaults

Use option 10 to load using the system default configuration and to boot without using the current startup configuration. Selecting 10 from the Boot Menu restores system defaults and deletes the configuration files. Boot Sequence can then be started by selecting 1 from the Boot Menu.

To download software from the **Boot** menu:

1. On the **Boot** menu, select **10** and press <Enter>.

   The following prompt displays:

   ```
   Are you SURE you want to delete the configuration? (y/n):y
   ```

2. The boot process resumes.

Activate Backup Image

Use option 11 to activate the backup image. The active image becomes the backup when this option is selected.

To activate the backup image:

1. From the **Boot** menu, select **11** and press <Enter>.

   The following message displays:

   ```
   Backup image - image2 activated.
   ```

2. The boot process resumes.

Downloaded from www.Manualslib.com manuals search engine

Password Recovery Procedure

Use option 12 when a password is lost. This allows the switch to boot one time without prompting for a console password. Note that the *enable* password is not prompted for in this mode.

To recover a lost password for the local terminal only:

1. From the **Boot** menu, select **12** and press <Enter>.

   The password is deleted.

2. The boot process resumes.
3. To ensure switch security, reconfigure passwords for applicable management methods.

Sample Configuration Process

This section provides the basic steps required to establish a remote network management connection with the switch. This section does not explain the various configurations available on the switch or the relevant commands.

This section also describes accessing a switch for the first time with the default configuration and definitions. If a previously entered configuration causes problems, the startup-configuration file — which is the configuration of switch when powered up — should be erased and the switch rebooted. See "Device Default Settings."

Switch Setup Requirements

The following components are required for the purpose of this example:

- PowerConnect M6220/M6348/M8024 switch
- A workstation with the following components installed:
  - Network adapter card
  - ASCII terminal application (for example, Microsoft® Windows® HyperTerminal or Procomm Plus™ Terminal)
  - A browser application
- The supplied serial cable

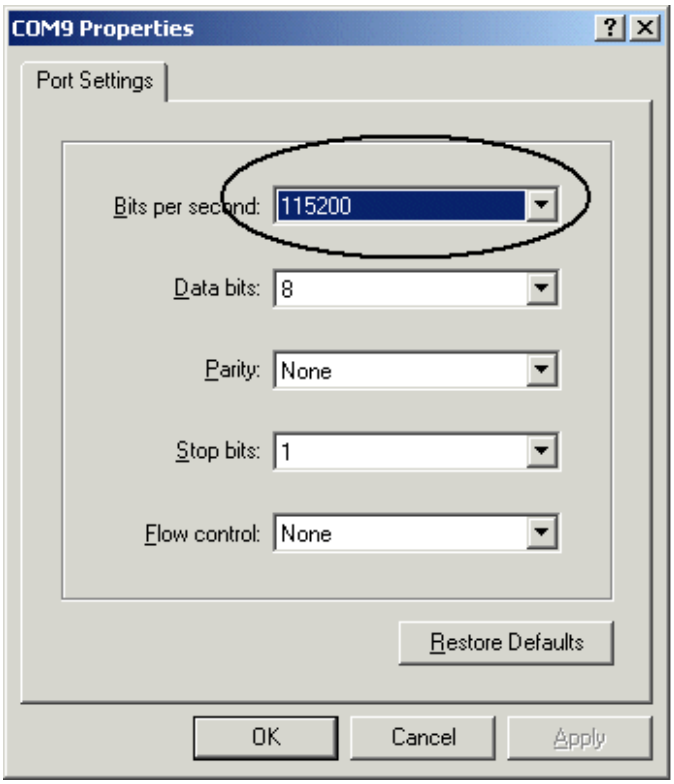
Downloaded from www.Manualslib.com manuals search engine

Initial Connection

1. Using the RS-232 port, connect the switch to the workstation.
2. Set the ASCII terminal with the following settings and select the appropriate COM port.

   The sample screen uses the HyperTerminal.

Figure 5-3. HyperTerminal Properties Window



Note: 9600 is the default baud rate for a new switch. The switch may have another baud rate. If using the default baud rate does not result in viewing the switch terminal, try another baud rate.

3. Use the provided serial cable to connect the workstation to the switch.
4. Connect the switch power cord and power up the switch. The system begins the boot process. When the following displays, you can enter the **Boot** menu by selecting **2**, if necessary, to run special procedures.

```
Select an option. If no selection in 10 seconds then operational code
will start.

1 - Start operational code.

2 - Start Boot Menu.

Select (1, 2):2
```


Downloaded from www.Manualslib.com manuals search engine

If you do not enter the **Boot** menu, the system continues operation by decompressing the code into RAM. The code starts running from the RAM and the list of available port numbers and their states (up or down) are displayed.

Note: The following screen is an example configuration. Items such as addresses, versions, and dates may differ for each switch.

```
current volume configuration:
 - volume label:    NO LABEL ; (in boot sector:              )
 - volume Id:       0x0
 - total number of sectors:   124,408
 - bytes per sector:     512
 - # of sectors per cluster: 4
 - # of reserved sectors:    1
 - FAT entry size:      FAT16
 - # of sectors per FAT copy:    122
 - # of FAT table copies:   2
 - # of hidden sectors:      8
 - first cluster is in sector #  260
 - Update last access date for open-read-close = FALSE
 - directory structure:         VFAT
 - file name format:            8-bit (extended-ASCII)
 - root dir start sector:               245
 - # of sectors per root:               15
 - max # of entries in root:            240

FAT handler information:
------------------------
 - allocation group size:       4 clusters
 - free space on volume:        44,380,160 bytes
```


Downloaded from www.Manualslib.com manuals search engine

```
Boot Menu Version: 12 May 2009
Select an option. If no selection in 10 seconds then
operational code will start.

1 - Start operational code.
2 - Start Boot Menu.
Select (1, 2):


Operational Code Date: Tue May 26 14:12:20 2009
Uncompressing.....

Target Name: vxTarget
Attached IPv4 interface to motetsec unit 0

Adding 70447 symbols for standalone.
 CPU: Broadcom SBC8548.  Processor #0.
 Memory Size: 0x20000000.  BSP version 2.0/2.
 Created: May 26 2009, 13:11:31
 ED&R Policy Mode: deployed
 WDB Comm Type: WDB_COMM_END
 WDB: Ready.
remLib: Not initialized.
remLib: Not initialized.
CFI Probe: Found 2x16 devices in x16 mode

volume descriptor ptr (pVolDesc):    0x706d770
XBD device block I/O handle: 0x10001
auto disk check on mount:      NOT ENABLED
```


Downloaded from www.Manualslib.com manuals search engine

```
volume write mode:         copyback (DOS_WRITE)
max # of simultaneously open files:    52
file descriptors in use:       0
# of different files in use:       0
# of descriptors for deleted files:    0
# of  obsolete descriptors:        0

current volume configuration:
 - volume label:    NO LABEL ; (in boot sector:              )
 - volume Id:       0x0
 - total number of sectors:   124,408
 - bytes per sector:     512
 - # of sectors per cluster: 4
 - # of reserved sectors:    1
 - FAT entry size:      FAT16
 - # of sectors per FAT copy:    122
 - # of FAT table copies:   2
 - # of hidden sectors:      8
 - first cluster is in sector #  260
 - Update last access date for open-read-close = FALSE
 - directory structure:         VFAT
 - file name format:            8-bit (extended-ASCII)
 - root dir start sector:               245
 - # of sectors per root:               15
 - max # of entries in root:            240

FAT handler information:
------------------------
 - allocation group size:       4 clusters
```


Downloaded from www.Manualslib.com manuals search engine

```
 - free space on volume:        44,380,160 bytes


PCI unit 0: Dev 0xb624, Rev 0x12, Chip BCM56624_B1, Driver
BCM56624_B0

SOC unit 0 attached to PCI device BCM56624_B1

Adding BCM transport pointers

Configuring CPUTRANS TX

Configuring CPUTRANS RX

st_state(0) = 0x0

st_state(1) = 0x2


<186> JAN 01 00:00:15 0.0.0.0-1 UNKN[536870176]: bootos.c(218) 1 %
Event(0xaaaaaaaa)

Instantiating RamCP: as rawFs,  device = 0x20001

Formatting RamCP: for DOSFS

Instantiating RamCP: as rawFs, device = 0x20001

Formatting...OK.


(Unit 1 - Waiting to select management unit)>


Applying Global configuration, please wait ...


Applying Interface configuration, please wait ...



console>
```


Downloaded from www.Manualslib.com manuals search engine

Device Default Settings

To return to device default settings use `delete startup-config` command at the privileged mode prompt (#), and reboot the device. Once device reloads – it is set with the default settings.

```
console>
console>enable
console#delete startup-config
Startup file was deleted
console#reload
Management switch has unsaved changes.
Are you sure you want to continue? (y/n) y

Configuration Not Saved!
Are you sure you want to reload the stack? (y/n) y

Reloading all switches..
```

Enabling Remote Management

1. Enter the **enable** command at the console to enter the Privileged EXEC screen mode as follows:

   ```
   console>enable
   console#
   ```

2. Ensure that the management station is connected to the same network as the CMC. For more info see the *Dell Blade Server CMC User's Guide.*
3. Enter the **config** command at the console to enter the Configuration mode as follows:

   ```
   console#config
   ```

4. Ensure that the switch has obtained an IP address using the **show ip interface out-of-band** command.

   ```
   console#show ip interface out-of-band

   IP Address..................................... 10.27.22.168
   Subnet Mask.................................... 255.255.255.0
   Default Gateway................................ 10.27.22.1
   ServPort Configured Protocol Current........... DHCP
   ```


Downloaded from www.Manualslib.com manuals search engine

```
Burned In MAC Address.......................... 0063.4802.0011


console#
```

5. Ping the management station from the switch to ensure that connectivity has been achieved.

   Wait 30 seconds for port to be in STP forwarding before pinging the management station. In this example, the Management station IP is 50.1.1.2.

```
console>ping 50.1.1.2

64 bytes from 50.1.1.2: icmp_seq=1. time=0 ms

64 bytes from 50.1.1.2: icmp_seq=2. time=0 ms

64 bytes from 50.1.1.2: icmp_seq=3. time=0 ms

64 bytes from 50.1.1.2: icmp_seq=4. time=0 ms


----50.1.1.2 PING Statistics----

4 packets transmitted, 4 packets received, 0% packet loss

round-trip (ms) min/avg/max = 0/0/0
```

6. Define a user name and password to allow privileged level 15 switch access for a remote user (HTTP and HTTPS).

   In this example, the user name **Dell**, the password is **Dell1234**, and the privilege level is 15. Privilege levels range from 1–15, with 15 being the highest level. Level 15 access is the only level of access for the Web interface.

```
console#config

console(config)#username Dell password Dell1234 level 15

console(config)#ip http authentication local

console(config)#ip https authentication local

console(config)#crypto certificate generate key_generate

Generating RSA private key, 1024 bit long modulus

console(config)#ip https server
```

7. Define a user name and password to allow access for a local user—console, Telnet, or Web Server, for example.

   In this example, the user name is **Dell, the password is Dell1234**, and the privilege level is 15.

```
console(config)#username Dell password Dell1234 level 15
```


Downloaded from www.Manualslib.com manuals search engine

```
console(config)#aaa authentication login default line
console(config)#aaa authentication enable default line
console(config)#line console
console(config-line)#login authentication default
console(config-line)#enable authentication default
console(config-line)#password tommy123
console(config-line)#exit
console(config)#line telnet
console(config-line)#login authentication default
console(config-line)#enable authentication default
console(config-line)#password bobby123
console(config-line)#exit
console(config)#line ssh
console(config-line)#login authentication default
console(config-line)#enable authentication default
console(config-line)#password jones123
console(config-line)#exit
```

8. Save the **running-config** file to the **startup-config** file.

   This ensures that the configuration just completed is the same if the switch is rebooted.

```
console(config)#exit
console#copy running-config startup-config
```

The switch is now configured and can be managed through the different options such as Telnet, Web browser interface, and others.

Downloaded from www.Manualslib.com manuals search engine

Configuring Secure Management Access (HTTPS)

When managing the switch securely through the standard Web browser, the SSL (Secure Socket Layer) security protocol is used.

To manage the switch securely through the standard Web browser, perform the following:

1. In order to configure the switch to allow HTTPS server, and to create a security key, use the commands **`ip https server`** and **`crypto certificate 1 generate`**:

   ```
   console#configure
   console(config)#crypto certificate 1 generate
   Generating RSA private key, 1024 bit long modulus
   console(config)#ip https server
   console(config)#
   ```

2. Configure the management station the same as for a regular HTTP connection.
3. Connect to the switch through HTTPS by typing the address `https://device IP address` in the browser window (*https* must be typed).

   The **Security Alert** window displays.
4. Click **Yes** to confirm accept the security certification (if it is not authenticated by a third party).

   The **Login Screen** displays.
5. Enter the assigned user name and password.

   The switch Dell OpenManage™ Switch Administrator displays.

Downloaded from www.Manualslib.com manuals search engine

6

Configuring System Information

Overview

Use the menus listed on the **System** page to define the switch's relationship to its environment. To display the **System** page, click **System** in the tree view. The **System** menu page contains links to the following features:

- Defining General Device Information
- Configuring SNTP Settings
- Managing Logs
- Setting the Operational Mode
- Defining IP Addressing
- Running Cable Diagnostics
- Managing Device Security
- Captive Portal
- Defining SNMP Parameters
- File Management
- Defining Advanced Settings
- Defining StackingsFlow
- Industry Standard Discovery Protocol

Downloaded from www.Manualslib.com manuals search engine

Defining General Device Information

The **General** menu page contains links to pages that allow you to configure device parameters. Use this page to access the following features:

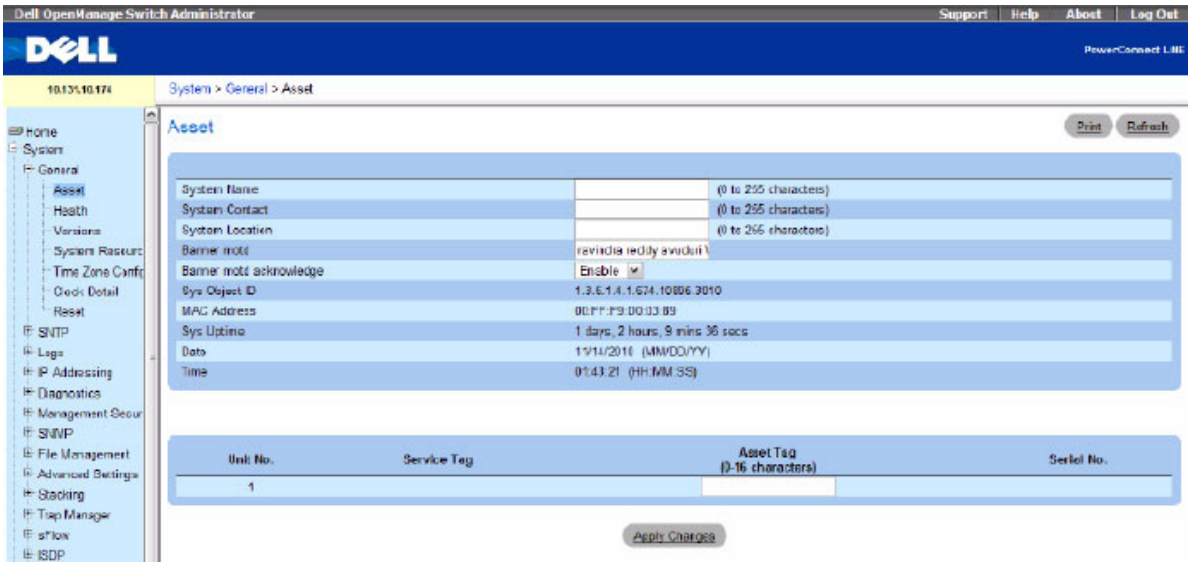
- Asset
- System Health
- Versions
- System Resources
- Time Zone Configuration
- Summer Time Configuration
- Clock Detail
- Reset

Asset

Use the **Asset** page fields to configure and view general device information.

To display the **Asset** page, click **System** > **General** > **Asset** in the tree view.

Figure 6-1. Asset



The **Asset** page contains the following fields:

- **System Name (0 – 255 characters)** — Use to assign device system name.
- **System Contact (0 – 255 characters)** — Use to assign the contact person's name.
- **System Location (0 – 255 characters)** — Use to specify a system location.

Downloaded from www.Manualslib.com manuals search engine

- **Banner motd (message of the day)** — Enter the message that appears on the GUI banner (if enabled).
- **Banner motd acknowledge** — Enable to display the GUI banner motd in the GUI banner.
- **Sys Object ID** — The assigned System Object ID.
- **MAC Address** — Displays the MAC address of the switch.
- **Sys Uptime** — Displays the number of days, hours, and minutes since the last restart.
- **Date** — Displays the current system date. The format is month, day, year (MM/DD/YY). For example, 11/01/05 is November 01, 2005.
- **Time** — Displays the current system time. The format is hour, minute, second (HH:MM:SS). For example, 20:12:03 is 8:12:03 PM.
- **Unit No.** — Displays the switch's position in the stack.
- **Service Tag** — Displays the service reference number used when servicing the device.
- **Asset Tag (0 – 16 characters)** — Displays the user-defined device reference.
- **Serial No.** — Displays the device serial number.

Defining System Information

1. Open the **Asset** page.
2. Define the following fields: **System Name**, **System Contact**, **System Location**, and **Asset Tag**.
3. Click **Apply Changes**.

   The system parameters are applied, and the device is updated.

Initiating a Telnet Session

1. Open the **Asset** page.

   Note: The appropriate telnet parameters are set prior to initiating the telnet session. See "Configuring an Initial Telnet Password" for information. If the client has a Microsoft® Windows® environment, the program must be configured for telnet. If the client has a Unix environment, the telnet program must exist in the path.

2. Click **Telnet**.

   The prompt appears, indicating that the system is ready to receive input.

Configuring Device Information Using the CLI Commands

For information about the CLI commands that perform this function, see the following chapters in the *CLI Reference Guide*:

- System Management Commands
- SNMP Commands
- Clock Commands

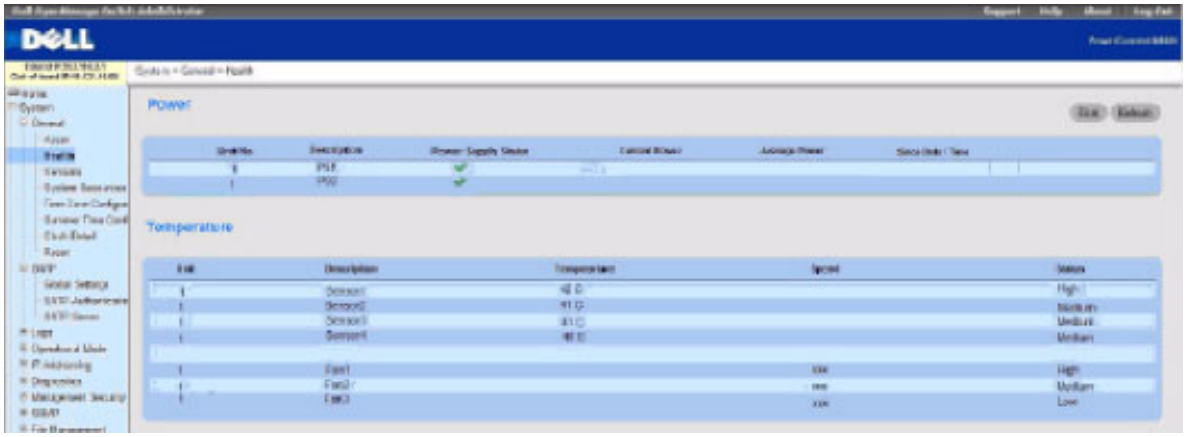
Downloaded from www.Manualslib.com manuals search engine

System Health

Use the **Health** page to view physical device information, including information about the switch's power and ventilation sources.

To display the **Health** page, click **System** > **General** > **Health** in the tree view.

Figure 6-2. Health



The **Health** page contains the following fields:

- **Unit No.** — Displays the unit's position in the stack.
- **Power Supply Status** — Displays the power supply status.
  - — The power supply is operating normally.
  - — The power supply is not operating normally.
  - **Not Present** — The power supply is currently not present.
- Average **Power**—Indicates the average power consumption since the date/time of the last bootup or calculation reset.
- **Fan Status**— Indicates the fan status. The PowerConnect 8024/8024FM6348 has three fans.
  - — The fan is operating normally.
  - — The fan is not operating normally.
  - **Not Present** — A fan is currently not present.
- **Temperature** — Displays the temperature at which the device is currently running.

Viewing System Health Information Using the CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- System Management Commands

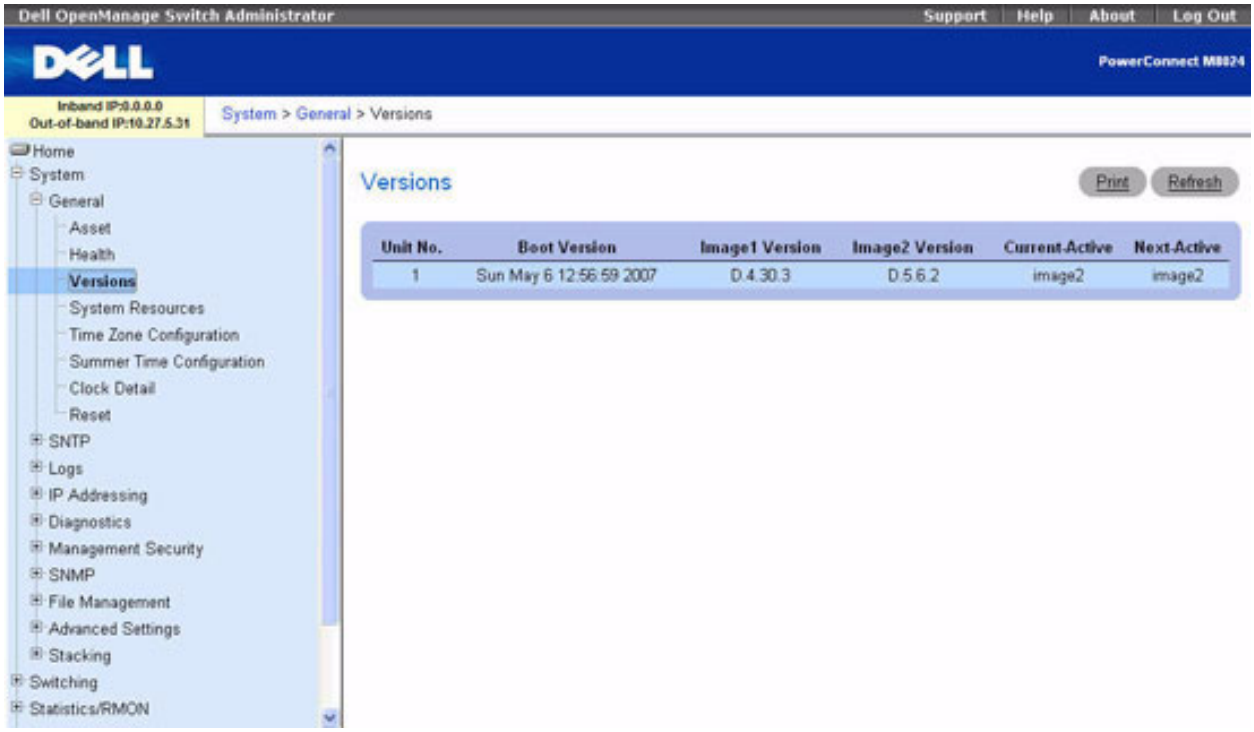
Downloaded from www.Manualslib.com manuals search engine

Versions

Use the **Versions** page to view information about the software versions currently running.

To display the **Versions** page, click **System** > **General** > **Versions** in the tree view.

Figure 6-3. Versions



The **Versions** page contains the following fields:

- **Unit No.** — Displays the unit's number in the stack.
- **Boot Version** — Displays the version of the boot code.
- **Image1 Version** — Displays the version number of one of the two available software images.
- **Image2 Version** — Displays the version number of the other of the two available software images.
- **Current-Active** — Displays the currently active software image.
- **Next-Active** — Displays the software image which will be loaded the next time the switch is rebooted.

Displaying Device Versions Using the CLI

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- System Management Commands

Downloaded from www.Manualslib.com manuals search engine

System Resources

Use the **System Resources** page to view information about memory usage and task utilization.

To display the **System Resources** page, click **System** > **General** > **System Resources** in the tree view.

Figure 6-4. System Resources

System Resources

Print Refresh

Memory Usage

Total Memory	524288 KBytes
Available Memory	59094016 KBytes

Task Utilization Report

Task Name	5 Seconds	1 Minute	5 Minutes
tNetTask	00.00	00.00	00.01
tIomEvtMon	02.00	01.54	01.15
osapiTimer	00.40	00.47	00.50
bcmL2X.0	00.00	00.39	00.49
bcmCNTR.0	00.80	00.73	00.79
bcmRX	00.00	00.17	00.30
bcmNHOP	00.00	00.00	00.01
bcmATP-RX	00.00	00.06	00.01
bcmLINK.0	00.00	00.28	00.31
osapiMonTask	00.00	00.00	00.08
tEmWeb	00.00	00.38	00.13
cmgrTask	00.00	00.00	00.01
DHCP snoop	00.00	00.00	00.02
Dynamic ARP Inspection	00.00	00.06	00.02
dot1s_timer_task	00.00	00.09	00.02
spmTask	00.00	00.00	00.05
tRipTask	00.00	00.00	00.01
pktRcvrTask	00.00	00.00	00.01
lldpTask	00.80	00.21	00.31
RMONTask	00.40	00.13	00.10

The **System Resources** page contains the following fields:

- **Total Memory** — Displays the total memory present on the switch.
- **Available Memory** — Displays the available memory (Free for allocation) present on the switch.
- **Task Name** — Name of the active task running on the switch.
- **Utilization (%)** — Percentage of CPU utilized by the corresponding task in the last:
  - Five seconds

Downloaded from www.Manualslib.com manuals search engine

– One minute
– Five minutes

Displaying System Resources Using the CLI

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

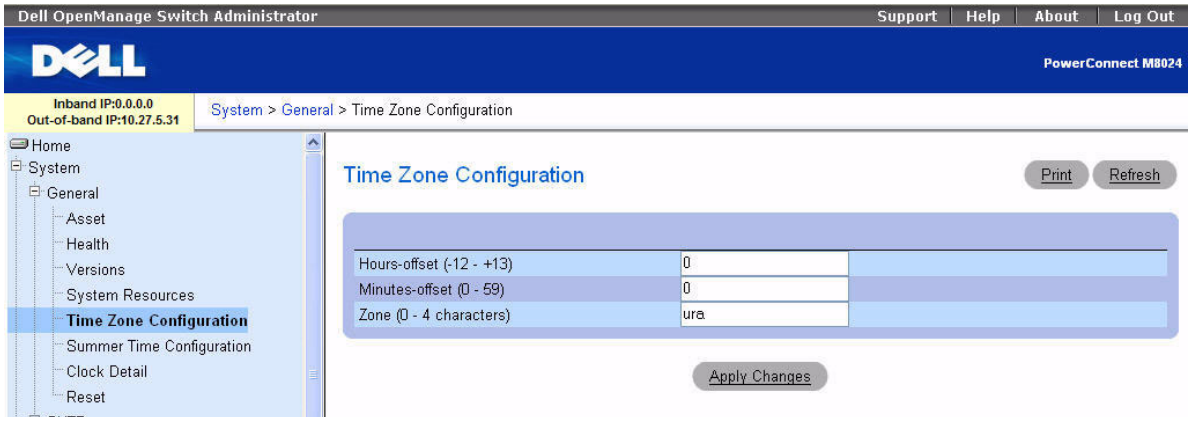
- System Management Commands

Time Zone Configuration

Use the **Time Zone Configuration** to configure the time zone difference from Coordinated Universal Time (UTC).

To display the **Time Zone Configuration** page, click **System > General > Time Zone Configuration** in the tree view.

Figure 6-5. Time Zone Configuration



The **Time Zone Configuration** page contains the following fields:

- **Hours-offset** — Set the hours difference from UTC. (Range: -12 to +13)
- **Minutes-offset** — Set the minutes difference from UTC. (Range: 0–59)
- **Zone** — Set the acronym of the time zone. (Range: 0–4 characters)

Defining the Time Zone Parameters

1. Open the **Time Zone Configuration** page.
2. Define the fields as needed.
3. Click **Apply Changes**.

   The time zone settings are modified, and the device is updated.

Downloaded from www.Manualslib.com manuals search engine

Configuring Time Zone Settings Using the CLI

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

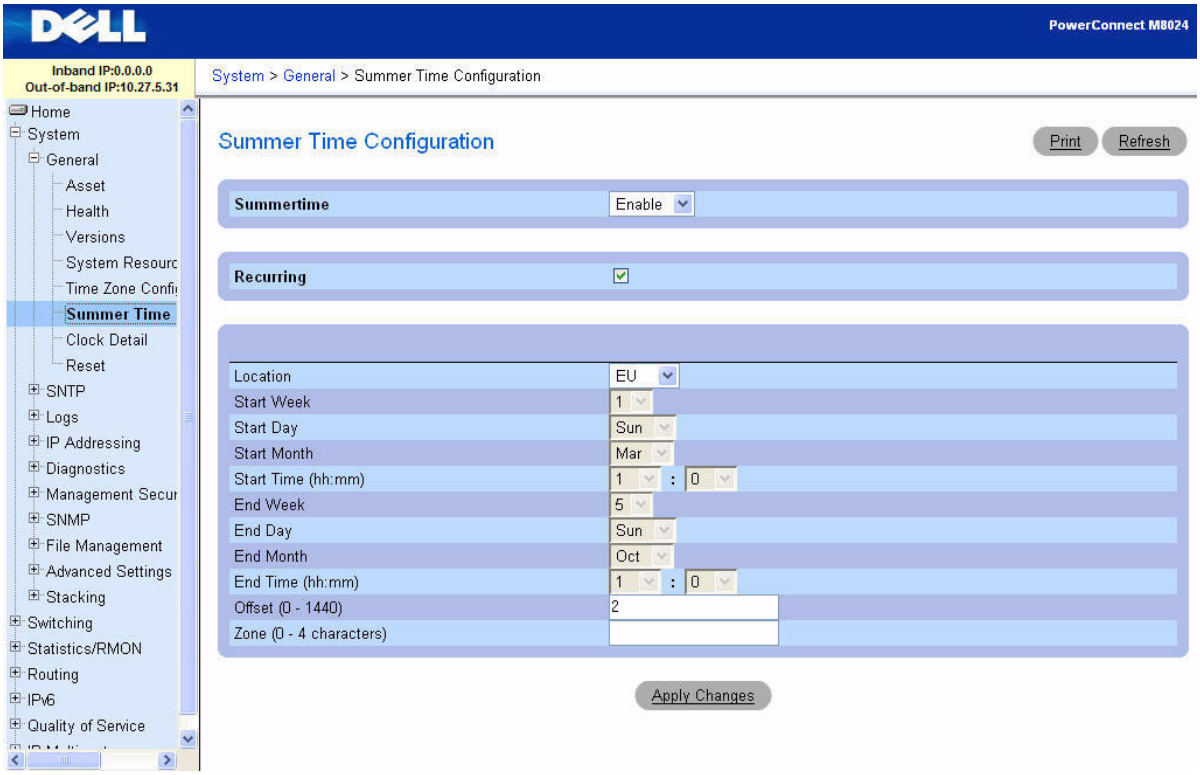
- Clock Commands

Summer Time Configuration

Use the **Summer Time Configuration** page to specify a defined summer time duration and offset.

To display the **Summer Time Configuration** page, click **System** > **General** > **Summer Time Configuration** in the tree view.

Figure 6-6. Summer Time Configuration



The fields on the **Summer Time Configuration** page change when you select or clear the Recurring check box. The **Summer Time Configuration** page contains the following fields:

- **Recurring** — Select the check box to indicate that the configuration is to be repeated every year.
- **Location** — This field displays only when the Recurring check box is selected. The summer time configuration is predefined for the United States and European Union. To set the summer time for a location other than the USA or EU, select None.

Downloaded from www.Manualslib.com manuals search engine

- **Start Week** — Select the starting week number. This field displays only when the Recurring check box is selected.
- **Start Day** — Select the starting day number. This field displays only when the Recurring check box is selected.
- **Start Month** — Select the starting month.
- **Start Time** — Select the starting time in hh:mm format.
- **Start Date** — Select the starting date. This field displays only when the Recurring check box is cleared.
- **Start Year** — Select the starting year. This field displays only when the Recurring check box is cleared.
- **End Week** — Select the ending week number. This field displays only when the Recurring check box is selected.
- **End Day** — Select the ending day number. This field displays only when the Recurring check box is selected.
- **End Month** — Select the ending month.
- **End Time** — Select the ending time in hh:mm format.
- **End Date** — Select the ending date. This field displays only when the Recurring check box is cleared.
- **End Year**. — Select the ending year. This field displays only when the Recurring check box is cleared.
- **Offset** — Set the number of minutes to add during summer time in the range 0 to 1440.
- **Zone** — Set the acronym of the time zone to be displayed when summer time is in effect.

Defining the Summer Time Parameters

1. Open the **Summer Time Configuration** page.
2. Define the fields as needed.
3. Click **Apply Changes**.

   The summer time settings are modified, and the device is updated.

Configuring Summer Time Parameters Using the CLI

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- Clock Commands

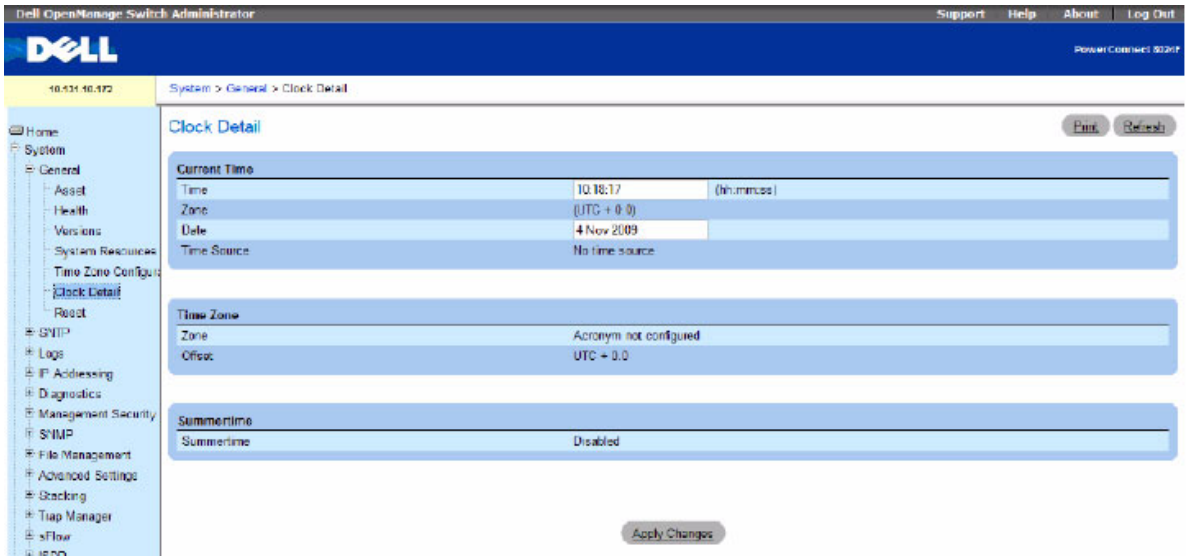
Downloaded from www.Manualslib.com manuals search engine

Clock Detail

Use the **Clock Detail** page to set the time and date or view information about the current time, time zone, and summer time settings.

To display the **Clock Detail** page, click **System** > **General** > **Clock Detail** in the tree view.

Figure 6-7. Clock Detail



The **Clock Detail** page provides information about the following clock features:

- **Current Time** — This section allows you to set the current time and date.
- **Time Zone** — This section displays the time zone settings.
- **Summertime** — This section displays the summer time settings.

Displaying Clock Detail Using the CLI

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- Clock Commands

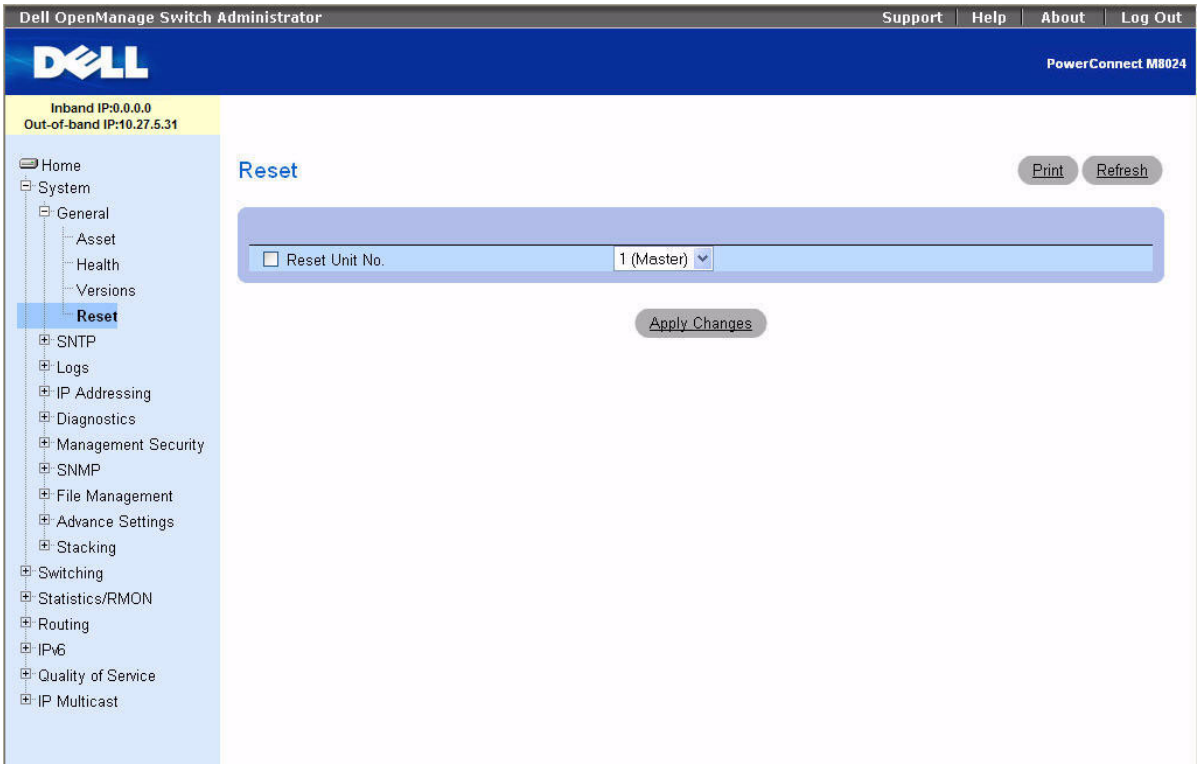
Downloaded from www.Manualslib.com manuals search engine

Reset

Use the **Reset** page to reset the device.

To display the **Reset** page, click **System** > **General** > **Reset** in the tree view.

Figure 6-8. Reset



The **Reset** page contains the following fields:

- **Reset Unit No.** — Use to select the device in the stack that needs to be reset.

Resetting the Device

1. Open the **Reset** page.
2. Click **Reset Unit No.**
3. Select either **Individual Unit** or **All.**
4. Click **Apply Changes** button.
5. When the confirmation message displays, click **OK**.

   The selected device is reset. After the device is reset, enter a user name and password.

Downloaded from www.Manualslib.com manuals search engine

Configuring SNTP Settings

The device supports the Simple Network Time Protocol (SNTP). SNTP assures accurate network device clock time synchronization up to the millisecond. Time synchronization is performed by a network SNTP server. The device operates only as an SNTP client and cannot provide time services to other systems.

Time sources are established by Stratums. Stratums define the accuracy of the reference clock. The higher the stratum (where zero is the highest), the more accurate the clock. The device receives time from stratum 1 and above since it is itself a stratum 2 device.

The following is an example of stratums:

- **Stratum 0** — A real time clock is used as the time source, for example, a GPS system.
- **Stratum 1 —** A server that is directly linked to a Stratum 0 time source is used. Stratum 1 time servers provide primary network time standards.
- **Stratum 2 —** The time source is distanced from the Stratum 1 server over a network path. For example, a Stratum 2 server receives the time over a network link, through NTP, from a Stratum 1 server.

Information received from SNTP servers is evaluated based on the time level and server type.

SNTP time definitions are assessed and determined by the following time levels:

- **T1** — Time at which the original request was sent by the client.
- **T2 —** Time at which the original request was received by the server.
- **T3** — Time at which the server sent a reply.
- **T4 —** Time at which the client received the server's reply.

The device can poll Unicast and Broadcast server types for the server time.

Polling for Unicast information is used for polling a server for which the IP address is known. SNTP servers that have been configured on the device are the only ones that are polled for synchronization information. T1 through T4 are used to determine server time. This is the preferred method for synchronizing device time because it is the most secure method. If this method is selected, SNTP information is accepted only from SNTP servers defined on the device using the **SNTP Servers** page.

Broadcast information is used when the server IP address is unknown. When a Broadcast message is sent from an SNTP server, the SNTP client listens to the message. If Broadcast polling is enabled, any synchronization information is accepted, even if it has not been requested by the device. This is the least secure method.

The device retrieves synchronization information, either by actively requesting information or at every poll interval. If Unicast and Broadcast polling are enabled, the information is retrieved in this order:

- Information from servers defined on the device is preferred. If Unicast polling is not enabled or if no servers are defined on the device, the device accepts time information from any SNTP server that responds.

Downloaded from www.Manualslib.com manuals search engine

- If more than one Unicast device responds, synchronization information is preferred from the device with the lowest stratum.
- If the servers have the same stratum, synchronization information is accepted from the SNTP server that responded first.

MD5 (Message Digest 5) Authentication safeguards device synchronization paths to SNTP servers. MD5 is an algorithm that produces a 128-bit hash. MD5 is a variation of MD4, and increases MD4 security. MD5 verifies the integrity of the communication, authenticates the origin of the communication.

The **SNTP** menu page contains links to pages that allow you to configure SNTP parameters.

To display the **SNTP** page, click **System > SNTP** in the tree view.

Use this page to go to the following features:

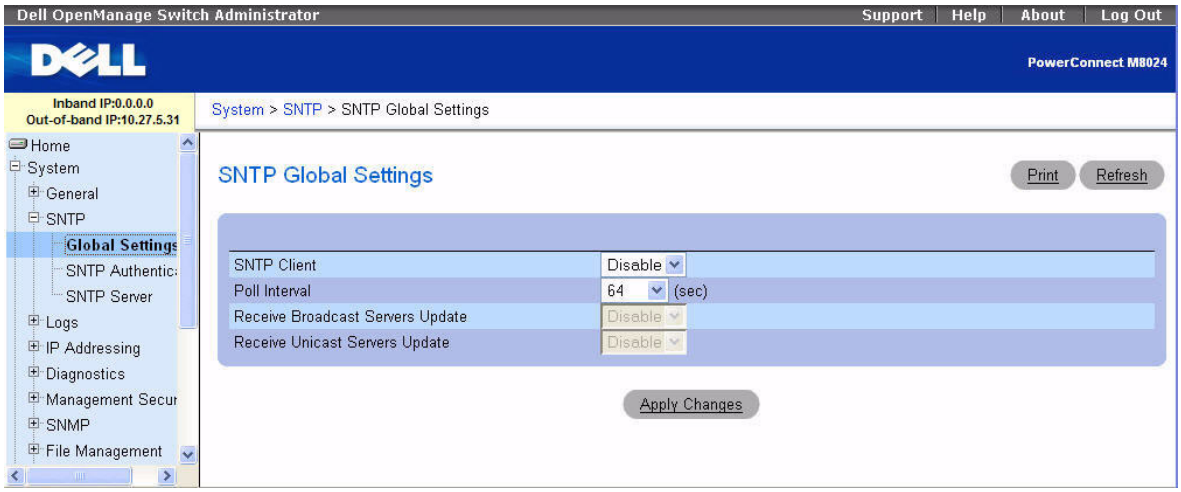
- SNTP Global Settings
- SNTP Authentication
- SNTP Server

SNTP Global Settings

Use the SNTP Global Settings page to view and adjust SNTP parameters.

To display the SNTP Global Settings page, click **System > SNTP > Global Settings** in the tree view.

Figure 6-9. SNTP Global Settings



The **SNTP Global Settings** page contains the following fields:

- **SNTP Client —** Use drop-down list to enable or disable the client. If the client is disabled, some of the fields below are also disabled.
- **Poll Interval —** Defines the interval (in seconds) at which the SNTP server is polled for Unicast information. The range is 60–1024 seconds.

Downloaded from www.Manualslib.com manuals search engine

- **Receive Broadcast Servers Update —** If enabled, listens to the SNTP servers for Broadcast server time information on the selected interfaces. The device is synchronized whenever an SNTP packet is received, even if synchronization was not requested.
- **Receive Unicast Servers Update —** If enabled, polls the SNTP servers defined on the device for Unicast server time information.

Defining SNTP Global Parameters

1. Open the **SNTP Global Settings** page.
2. Define the fields as needed.
3. Click **Apply Changes**.

   The SNTP global settings are modified, and the device is updated.

Defining SNTP Global Parameters Using CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- Clock Commands.

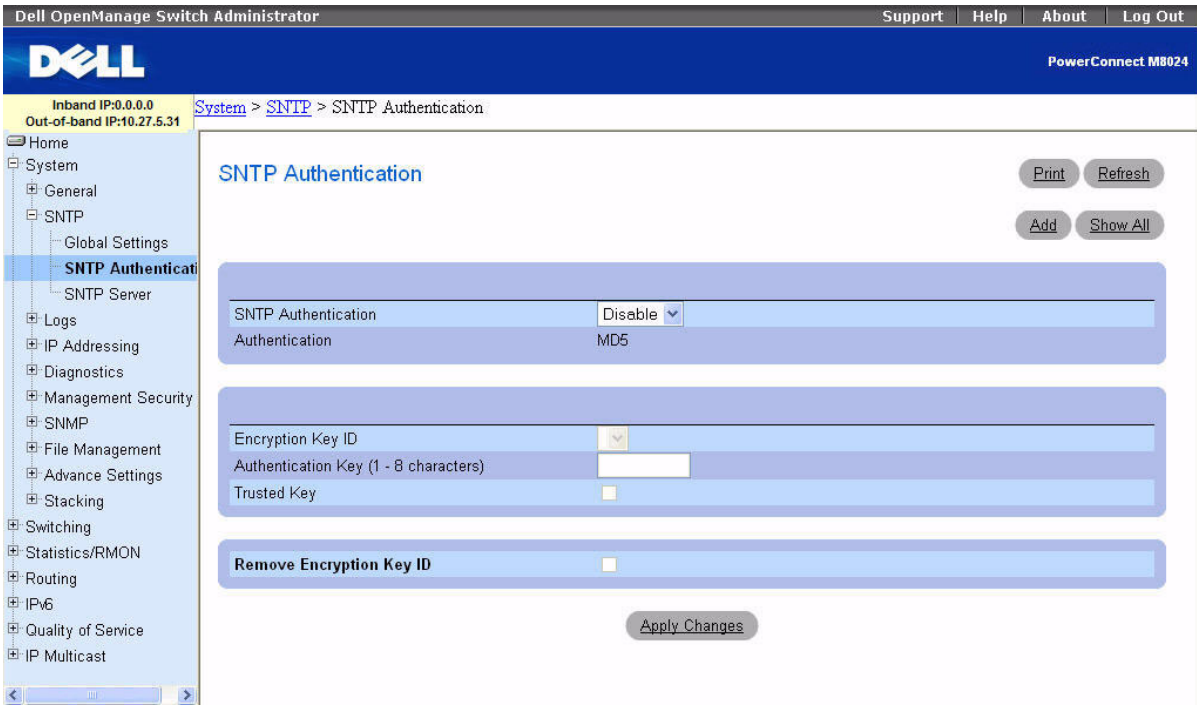
SNTP Authentication

The **SNTP Authentication** page lets you enable SNTP authentication between the device and an SNTP server, and to select the desired SNTP server. Use the **SNTP Authentication** page to enable or disable SNTP authentication, to modify the authentication key for a selected encryption key ID, to designate the selected authentication key as a trusted key, and to remove the selected encryption key ID.

Click **System** > **SNTP** > **Authentication** in the tree view to display the **SNTP Authentication** page.

Downloaded from www.Manualslib.com manuals search engine

Figure 6-10. SNTP Authentication



The **SNTP Authentication** page contains the following fields:

- **SNTP Authentication —** If enabled, requires authenticating an SNTP session between the device and an SNTP server.
- **Authentication —** Type of authentication. System supports MD5 only.
- **Encryption Key ID —** Contains a list of user-defined key IDs used to authenticate the SNTP server and device. Possible field values are 1–4294767295.
- **Authentication Key (1–8 Characters)** — Displays the key used for authentication.
- **Trusted Key —** Check to specify the encryption key used (Unicast) or uncheck to authenticate the SNTP server (Broadcast).
- **Remove Encryption Key ID —** Check to remove the selected authentication key.

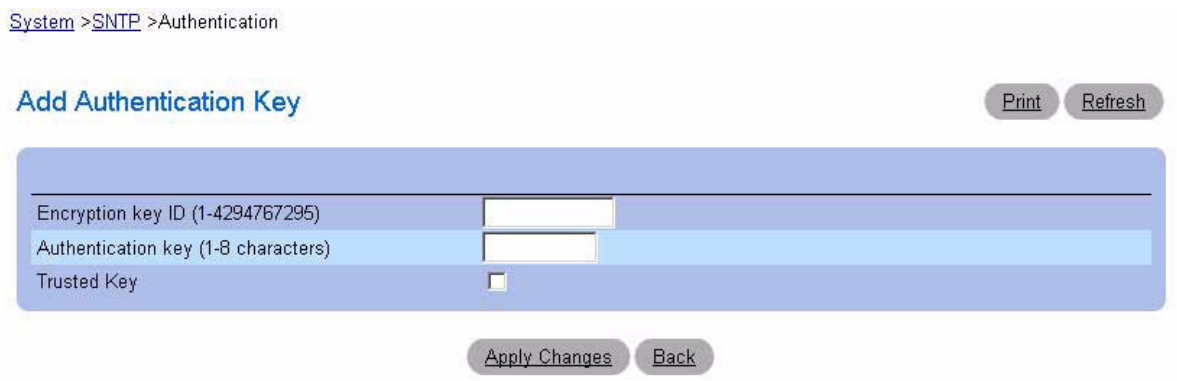
Downloaded from www.Manualslib.com manuals search engine

Adding an SNTP Authentication Key

1. Open the **SNTP Authentication** page.
2. Click **Add**.

   The **Add Authentication Key** page displays:

Figure 6-11. Add Authentication Key



3. Define the fields as needed.
4. Click **Apply Changes**.

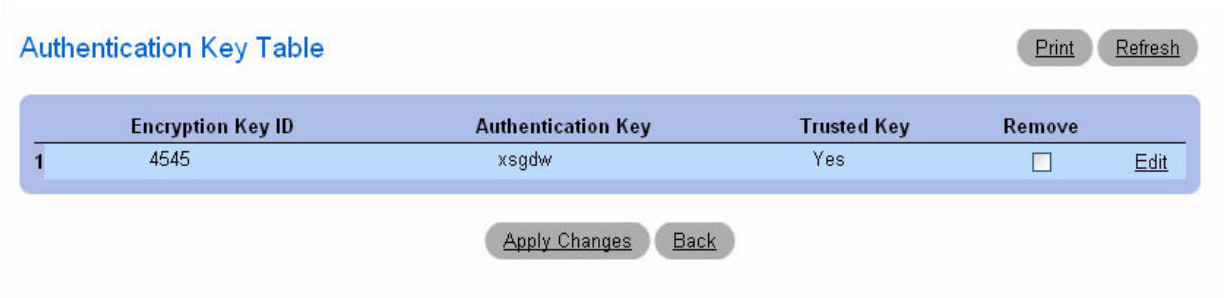
   The SNTP authentication key is added, and the device is updated.

Displaying the Authentication Key Table

1. Open the **SNTP Authentication** page.
2. Click **Show All**.

   The **Authentication Key Table** page displays:

Figure 6-12. Authentication Key Table



Downloaded from www.Manualslib.com manuals search engine

Removing an Authentication Key

1. Open the **SNTP Authentication** page.
2. Click **Show All**.

   The **Authentication Key Table** page displays.
3. Select an **Authentication Key Table** entry by checking its the **Remove** check box.
4. Click **Apply Changes**.

   The entry is removed, and the device is updated.

Defining SNTP Authentication Settings Using CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

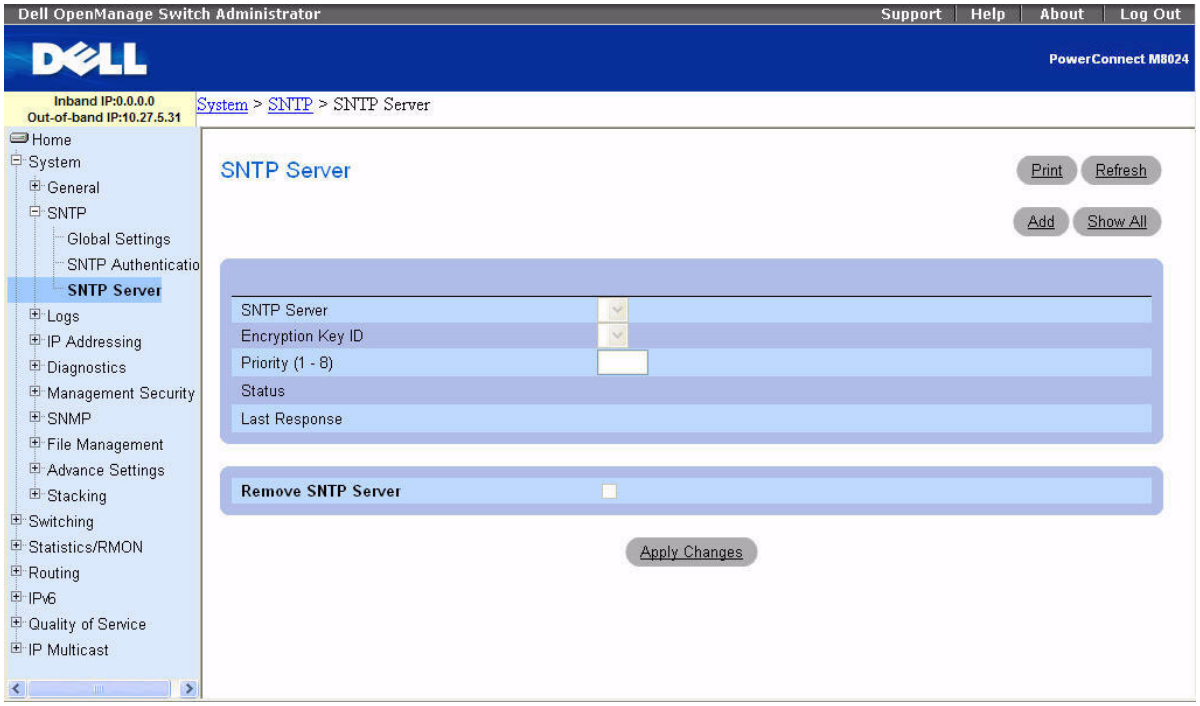
- Clock Commands.

SNTP Server

Use the **SNTP Server** page to view and modify information for enabling SNTP servers, and to add new SNTP servers.

To display the **SNTP Server** page, click **System** > **SNTP** > **SNTP Server** in the tree view.

Figure 6-13. SNTP Servers



Downloaded from www.Manualslib.com manuals search engine

The **SNTP Servers** page contains the following fields:

- **SNTP Server —** Selects user-defined SNTP server IP address from a drop-down menu. Up to eight SNTP servers can be defined by using the **Add** button.
- **Encryption Key ID —** Specifies user-defined key ID used to communicate between the SNTP server and device. The encryption key ID is defined in the **SNTP Authentication** page.
- Priority (1–8) — Specifies the priority of this server entry in determining the sequence of servers to which SNTP requests are sent. Values are 1 to 8, and the default is 1. Servers with lowest numbers have priority.
- **Status** — Displays the operating SNTP server status. The possible field values are:
  - **Up —** The SNTP server is currently operating normally.
  - **Down —** Indicates that a SNTP server is currently not available. For example, the SNTP server is currently not connected or is currently down.
  - **In progress —** The SNTP server is currently sending or receiving SNTP information.
  - **Unknown** — The progress of the SNTP information currently being sent is unknown. For example, the device is currently looking for an interface.
- **Last Response** — Displays the last time a response was received from the SNTP server.
- **Remove SNTP Server**— Removes a specified SNTP server from the **SNTP Servers** list when checked.

Adding an SNTP Server

1. Open the **SNTP Servers** page.
2. Click **Add.**

   The **Add SNTP Server** page displays.

Figure 6-14. Add SNTP Server

3. Define the fields as needed.
4. Click **Apply Changes**.

   The SNTP server is added, and the device is updated.

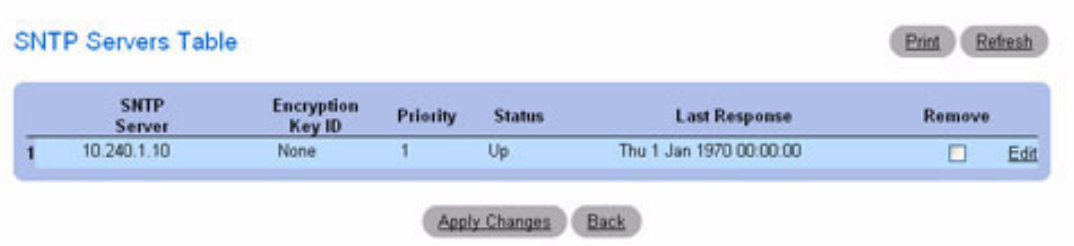
Downloaded from www.Manualslib.com manuals search engine

Displaying the SNTP Servers Table

1. Open the **SNTP Servers** page.
2. Click **Show All.**

   The **SNTP Servers Table** page displays.

Figure 6-15. SNTP Servers Table



Modifying an SNTP Server

1. Open the **SNTP Servers** page.
2. Click **Show All.**

   The **SNTP Servers Table** opens.
3. Click **Edit** next to the **SNTP Server** entry you wish to modify.
4. Modify the relevant fields.
5. Click **Apply Changes**.

   The SNTP server information is updated.

Removing the SNTP Server

1. Open the **SNTP Servers** page.
2. Click **Show All.**

   The **SNTP Servers Table** opens.
3. Select an **SNTP Server** entry.
4. Check the **Remove** check box.
5. Click **Apply Changes**.

   The entry is removed, and the device is updated.

Defining SNTP Servers Using CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

Downloaded from www.Manualslib.com manuals search engine

- Clock Commands.

Managing Logs

The switch may generate messages in response to events, faults, or errors occurring on the platform as well as changes in configuration or other occurrences. These messages are stored both locally on the platform and forwarded to one or more centralized points of collection for monitoring purposes as well as long term archival storage. Local and remote configuration of the logging capability includes filtering of messages logged or forwarded based on severity and generating component.

The *in-memory* log stores messages in memory based upon the settings for message component and severity.

The *persistent* log is stored in persistent storage. Two types of persistent logs may be configured.

- The first log type is the ***system startup log***. The system startup log stores the first N messages received after system reboot. This log always has the log full operation attribute set to stop on full and can store up to 32 messages.
- The second log type is the ***system operation log***. The system operation log stores the last N messages received during system operation. This log always has the log full operation attribute set to overwrite. This log can store up to 1000 messages.

Either the system startup log or the system operation log stores a message received by the log subsystem that meets the storage criteria, but not both. On system startup, if the startup log is configured, it stores messages up to its limit. The operation log, if configured, then begins to store the messages.

The system keeps up to three versions of the persistent logs, named <FILE>0.txt, <FILE>1.txt, and <FILE>2.txt. Upon system startup, <FILE>2.txt is removed, <FILE>1.txt is renamed <FILE>2.txt, <FILE>0.txt is renamed <FILE>1.txt, <FILE>0.txt is created and logging begins into <FILE>0.txt. (Replace <FILE> in the above example to specify `olog` for the operation log and `slog` for the startup log.)

The local persistent logs can be retrieved by using the CLI, xmodem over the local serial cable, and TFTP.

To display the **Logs** menu page, click **System** > **Logs** in the tree view. Use this page access the following features:

- Global Settings
- RAM Log Table
- Log File
- Remote Log Server Settings

Global Settings

Use the **Global Settings** page to enable logs globally, and to define log parameters. The **Severity** log messages are listed from the highest severity to the lowest.

Downloaded from www.Manualslib.com manuals search engine

To display the **Global Settings** page, click **System** > **Logs** > **Global Settings** in the tree view.

Figure 6-16. Global Settings

The **Global Settings** page contains the following fields:

- **Logging** — Enables device global logs for Cache, File, and Server Logs. All logs which are printed to the console are saved to the log files. The possible field values are:
  - **Enable —** Enables saving logs in Cache (RAM), File (FLASH), and an External Server.
  - **Disable** — Disables saving logs. It is not possible to disable logging of logs that are printed to console.

Severity

Use the check boxes in this section to adjust the sensitivity of the console, persistent memory, and log files.

When you select a specific level, all of the levels above it are automatically selected. For example, if you select Error, the system automatically selects Error, Critical, Alert, and Emergency. If you deselect Error, all of the levels below (for example, Error, Warning, Notice, Informational, Debug) are deselected.

- **Emergency** — The highest level warning level. If the device is down or not functioning properly, an emergency log is saved to the device.

Downloaded from www.Manualslib.com manuals search engine

- **Alert** — The second highest warning level. An alert log is saved if there is a serious device malfunction, such as all device features being down.
- **Critical —** The third highest warning level. A critical log is saved if a critical device malfunction occurs, for example, two device ports are not functioning, while the rest of the device ports remain functional.
- **Error** — A device error has occurred, such as if a port is offline.
- **Warning —** The lowest level of a device warning.
- **Notice** — Provides the network administrators with device information.
- **Informational** — Provides device information.
- **Debug —** Provides detailed information about the log. Debugging should only be entered by qualified support personnel.

The check boxes appear under the following three columns:

- **Console —** Logs sent to the console.
- **RAM Logs —** Logs sent to the (Cache) RAM.
- **Log File** — Logs sent to the File (FLASH).

Enabling Logs

1. Open the **Global Settings** page.
2. Select **Enable** in the **Logging** drop-down menu.
3. Use the check boxes to select log type and severity.

   Note: When you select a severity level, all higher severity levels are automatically selected.
4. Click **Apply Changes**.

   The log settings are saved, and the device is updated.

Enabling Global Logs Using the CLI

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- Syslog Commands.

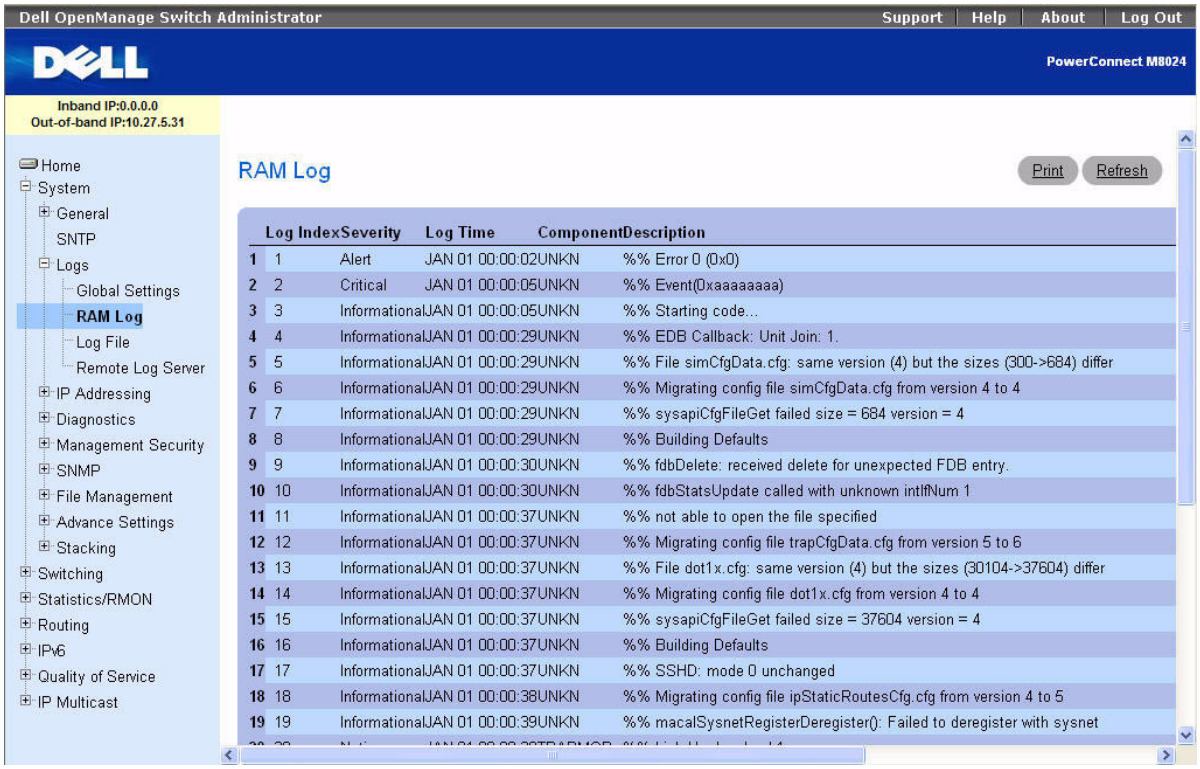
Downloaded from www.Manualslib.com manuals search engine

RAM Log Table

Use the **RAM Log Table** page to view information about specific RAM (cache) log entries, including the time the log was entered, the log severity, and a description of the log.

To display the **RAM Log Table**, click **System** > **Logs** > **RAM Log** in the tree view.

Figure 6-17. RAM Log Table



The **RAM Log Table** contains the following fields:

- **Log Index** — Indicates the Log Number within the Log RAM Table.
- **Severity** — The log severity.
- **Log Time** — The time at which the log was entered in the Log RAM Table.
- **Component** — The component being logged.
- **Description** — The log description.

Removing Log Information

1. Open the **RAM Log Table** page.
2. Click **Clear Log**.

   The log information is removed from the log file table, and the device is updated.

Downloaded from www.Manualslib.com manuals search engine

Removing Log Information Using the CLI

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

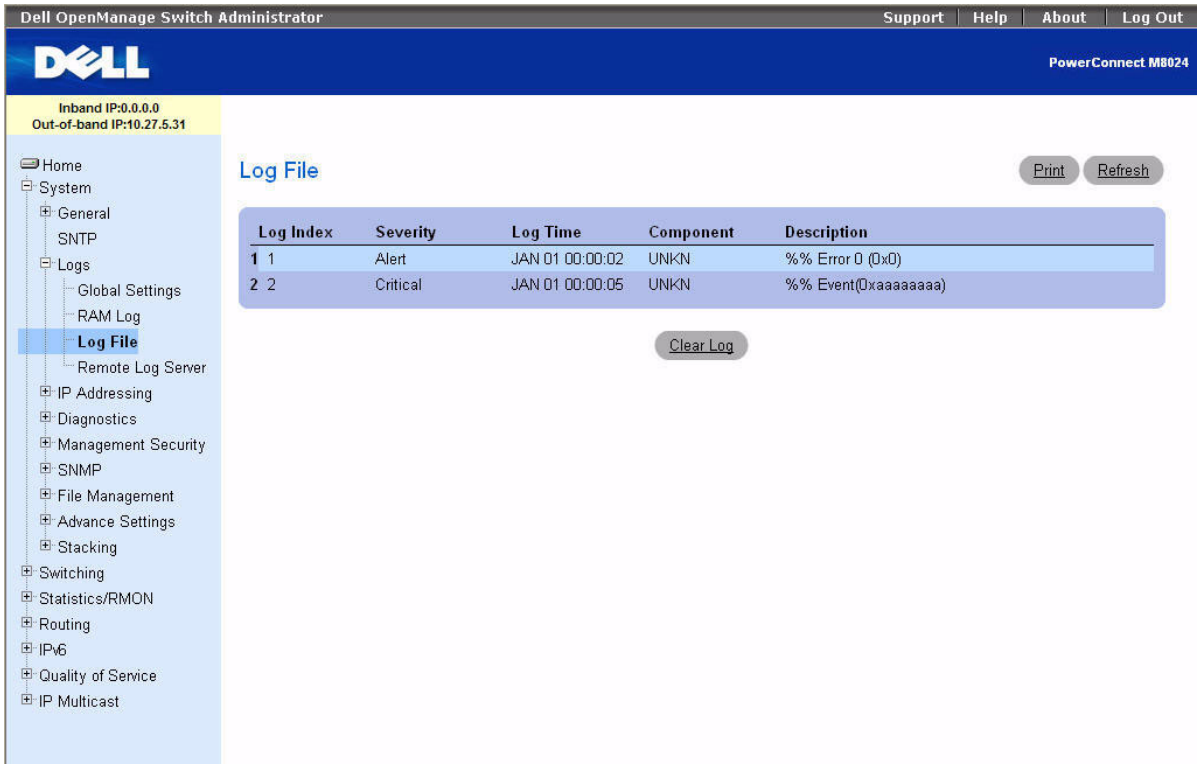
- Syslog Commands.

Log File

The **Log File** contains information about specific log entries, including the time the log was entered, the log severity, and a description of the log.

To display the **Log File**, click **System** > **Logs** > **Log File** in the tree view.

Figure 6-18. Log File



The **Log File Table** page contains the following fields:

- **Log Index** — The Log Number within the Log File Table.
- **Severity** — The log severity.
- **Log Time** — The time at which the log was entered in the Log File Table.
- **Component** — The component being logged.
- **Description** — The log description.

Downloaded from www.Manualslib.com manuals search engine

Removing Log Information

1. Open the **Log File Table** page.
2. Click **Clear Log**.

   The log information is removed from the log file table, and the device is updated.

Removing Log Information Using the CLI

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

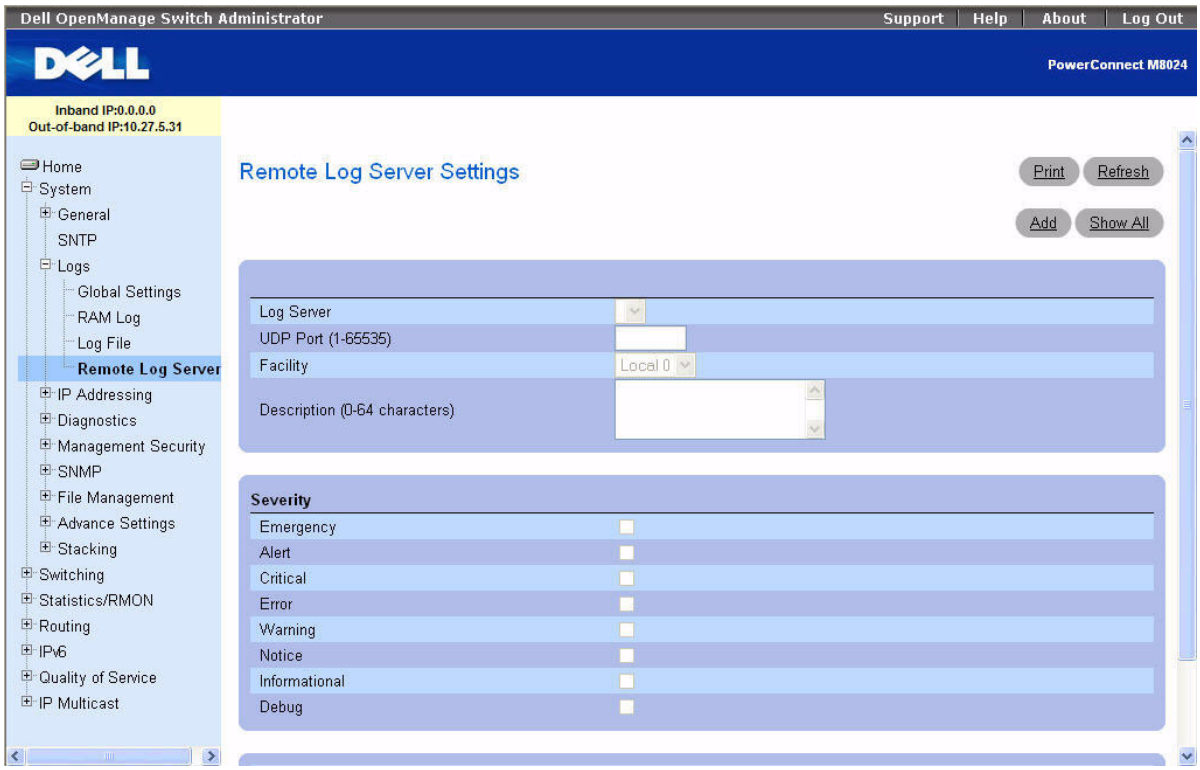
- Syslog Commands.

Remote Log Server Settings

Use the **Remote Log Server Settings** page to view the available log servers, to define new log servers, and to set the severity of the log events sent to the server.

To display the **Remote Log Server Settings** page, click **System** > **Logs** > **Remote Log Server**.

Figure 6-19. Remote Log Server Settings



The **Remote Log Server Settings** page contains the following fields:

- **Log Server** — Server to which logs can be sent.

Downloaded from www.Manualslib.com manuals search engine

- **UDP Port (1–65535) —** Sets the UDP port from which the logs are sent. The default value is 514.
- **Facility —** A user-defined application from which system logs are sent to the remote server. Only one facility can be assigned to a single server. If a second facility level is assigned, the first facility level is overridden. All applications defined for a device use the same facility on a server. The possible field values are from **Local 0** to **Local 7**.
- **Description** — Sets the server description. The maximum length is 64 characters.
- **Severity** — Selects the log severity. Selecting a severity level automatically selects all higher severity levels.
- **Remove Log Server** — Removes a server from the **Log Server** list. Checking the check box removes the server from the list. Leaving the box unchecked maintains the server in the list.

The **Remote Log Server Settings** page also contains a severity list. The severity definitions are the same as the severity definitions on the **RAM Log Table** page.

Sending Logs to a Server

1. Open the **Remote Log Server Settings** page.
2. Define the **UDP Port**, **Facility**, and **Description** fields.
3. Select the log type and log severity by using the **Log Parameters** check boxes.

   Note: When you select a severity level, all higher severity levels are automatically selected.
4. Click **Apply Changes**.

   The log settings are saved, and the device is updated.

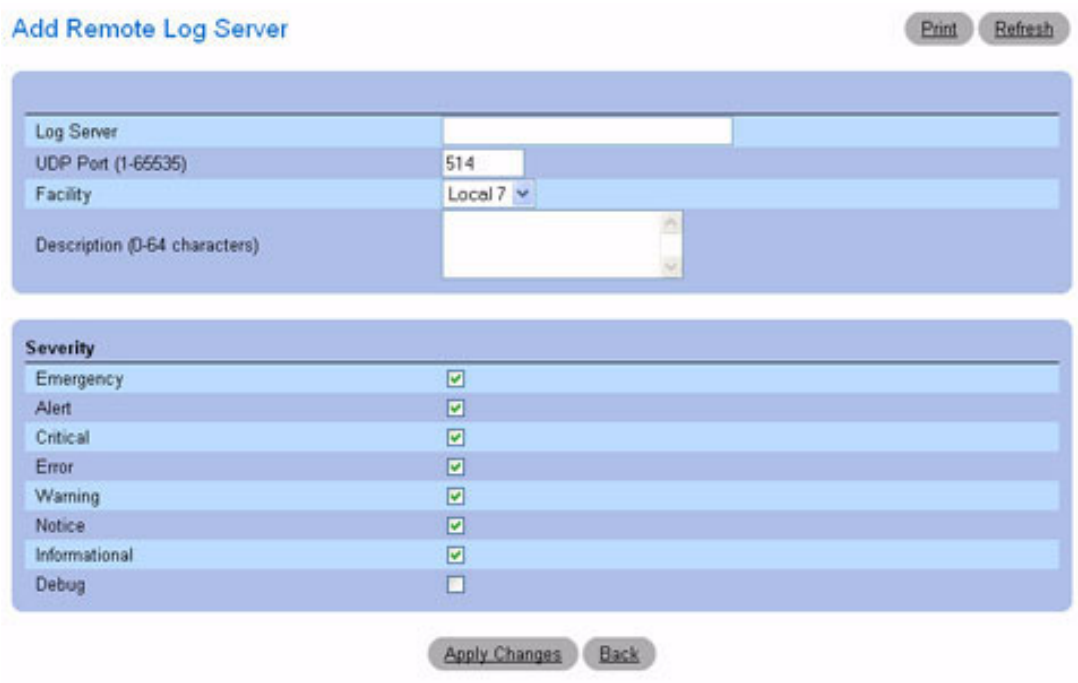
Adding a New Server

1. Open the **Remote Log Server Settings** page.
2. Click **Add** to display the **Add Remote Log Server** page.

   Note: Before adding a new server, determine the IP address of the remote log server.

Downloaded from www.Manualslib.com manuals search engine

Figure 6-20. Add Remote Log Server Settings



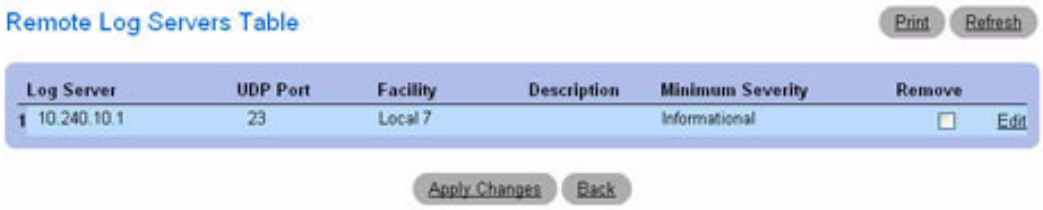
3. Complete the fields in the dialog and click **Apply Changes**.

   The **Remote Log Server Settings** page displays the server in the **Log Server** list only after you go back to the **Remote Log Server Settings** page.

Viewing/Removing a Log Server

1. Open the **Remote Log Server Settings** page.
2. Click **Show All** to display the **Remote Log Servers Table** page.

Figure 6-21. Show All Log Servers



3. To remove a server, check the corresponding **Remove** check box.
4. Click **Apply Changes**.

   The server is removed, and the device is updated.

Downloaded from www.Manualslib.com manuals search engine

Working with Remote Server Logs Using the CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- Syslog Commands.

Setting the Operational Mode

Users with a privilege level of 15 can configure the switch to operate in normal mode or simple mode. By default, the switch operates in normal mode. When the PowerConnect M6220/M6348/M8024 is operating in simple mode, a limited number of features are available to configure. For features that are not supported in simple mode, their administrative Web pages and CLI commands are hidden.

The following list shows the features that are available in Simple mode. Some configuration options with the listed features might not be available.

- Management Security (No Telnet Server or Denial of Service)
- File Management
- Port Status and Statistics (Ethernet ports only)
- Port Channel Status
- Dot1x
- SNMP
- SSH
- General System Information (Read-Only)
- HTTP Server
- Port Aggregator (Available **only** in Simple mode)

To display the **Operational Mode** menu page, click **System > Operational Mode** in the tree view. Use this page to go to the **Operational Mode Configuration** page.

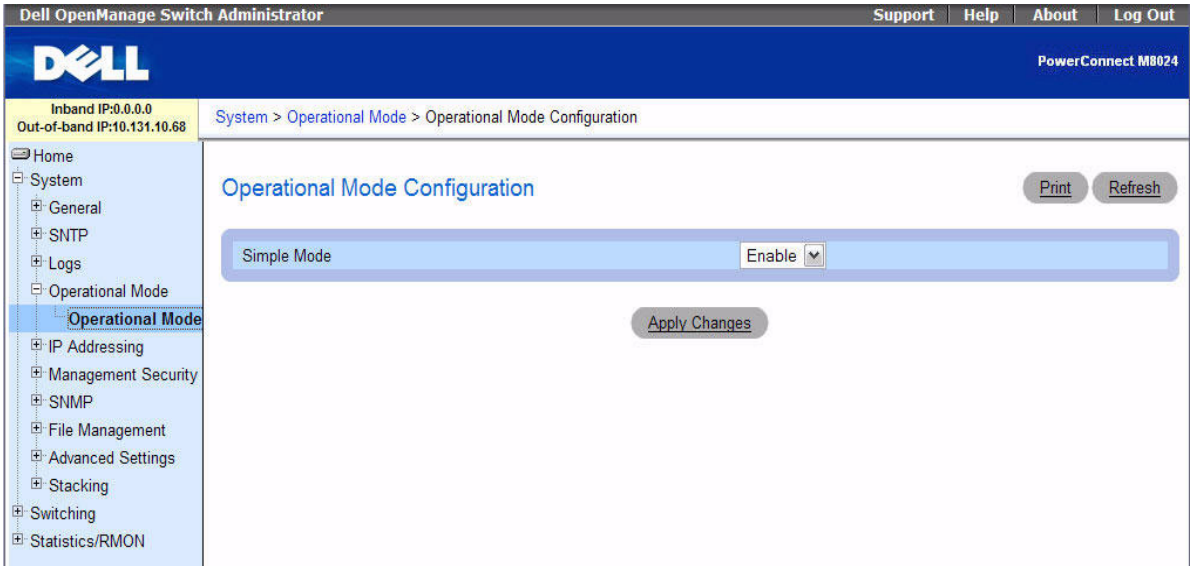
Operational Mode Configuration

Use the **Operational Mode Configuration** page to enable Simple mode or return the switch to normal mode. Only users with the highest privilege level can change the operating mode.

To display the **Operational Mode Configuration** page, click **System > Operational Mode > Operational Mode Configuration** in the tree view.

Downloaded from www.Manualslib.com manuals search engine

Figure 6-22. Operational Mode Configuration



The **Operational Mode Configuration** page contains the following fields:

- **Simple Switch Mode —** Enable or disable Simple mode on the switch. When Simple Switch Mode is disabled, the switch operates in the normal mode, and all applicable features described in this User's Guide are visible. When Simple Switch Mode is enabled, many of the features described in this document are hidden and unavailable.

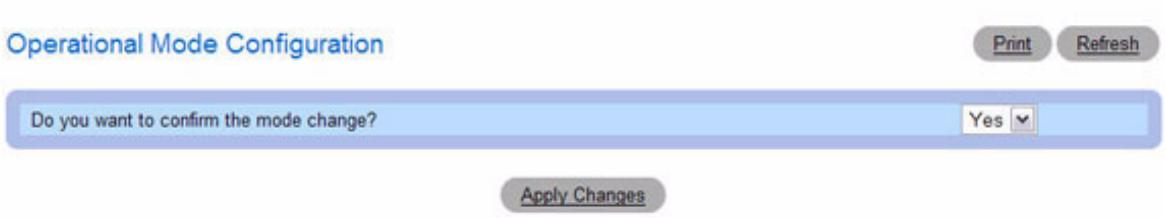
Configuring the Operational Mode

1. Open the **Operational Mode Configuration** page.
2. Select the appropriate option to enable or disable the Simple Switch Mode.
3. Click **Apply Changes**.

   The screen refreshes, and the **Operational Mode Configuration Confirmation** page displays. After the confirmation page displays, you must confirm the mode change within 60 seconds in order to continue.

Downloaded from www.Manualslib.com manuals search engine

Figure 6-23. Operational Mode Configuration Confirmation



4. To confirm the mode change, select **Yes**.
5. Click **Apply Changes** to change the mode.

Changing the Operating Mode Using the CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- Operational Mode Commands

Defining IP Addressing

Use the **IP Addressing** page to assign management interface and default gateway IP addresses, negotiate with the Domain Name System, set a Default Domain Name, perform Host Name Mapping, and define ARP and DHCP parameters for the interfaces.

To display the **IP Addressing** page, click **System > IP Addressing** in the tree view. Use this page to go to the following features:

- Out of Band Interface
- Domain Name Server (DNS)
- Default Domain Name
- Host Name Mapping
- Dynamic Host Name Mapping
- ARP Table
- IPv6 Management Features

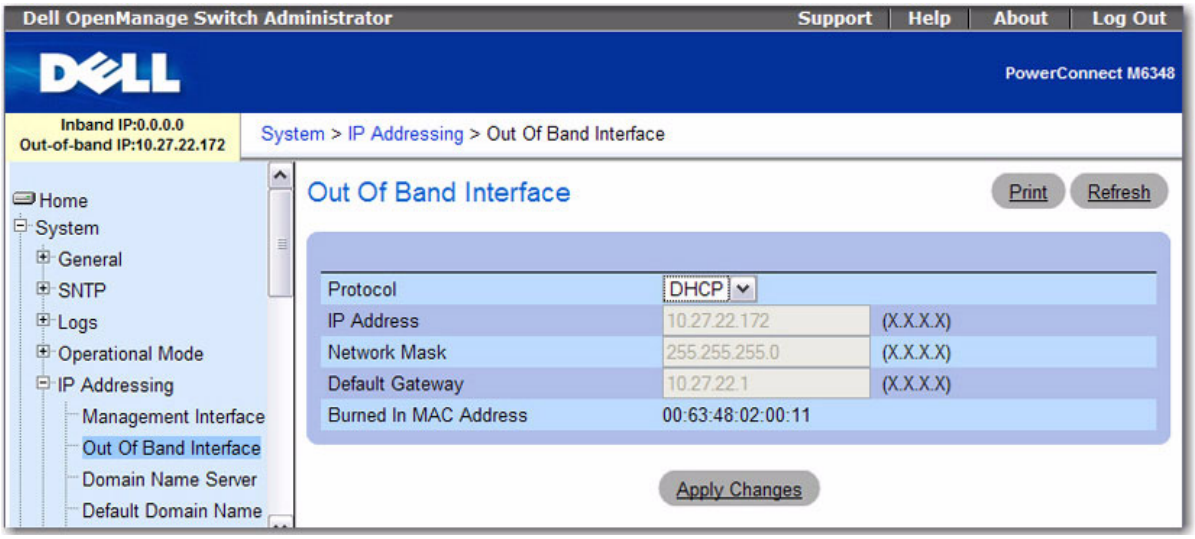
Downloaded from www.Manualslib.com manuals search engine

Out of Band Interface

Use the **Out of Band Interface** menu page to assign the Out of Band Interface IP address, the Subnet Mask, the Default Gateway IP address, and to assign the boot protocol.

To display the **Out of Band Interface** page, click **System > IP Addressing > Out of Band Interface** in the tree view.

Figure 6-24. Out of Band Interface



The **Out of Band Interface** page contains the following fields:

- **Protocol** — Use the drop-down menu to select None, Bootp, or DCHP.
- **IP Address —** Displays the Out of Band Interface IP address.
- **Network Mask** — The subnet mask of the source IP address.

  Note: Each part of the IP address must start with a number other than zero. For example, IP addresses 001.100.192.6 and 192.001.10.3 are not valid.
- **Default Gateway** — Sets the default gateway IP address.
- **Burned in MAC Address** — Displays the Burned in MAC Address of the Out of Band Interface.

Modifying Out of Band Interface IP Address Parameters

1. Open the **Out of Band Interface** page.
2. Modify the IP address in the **IP Address** field.
3. Modify other fields as needed.
4. Click **Apply Changes**.

   The parameters are modified, and the device is updated.

Downloaded from www.Manualslib.com manuals search engine

Defining Out of Band Interface Parameters Using CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- IP Addressing Commands.

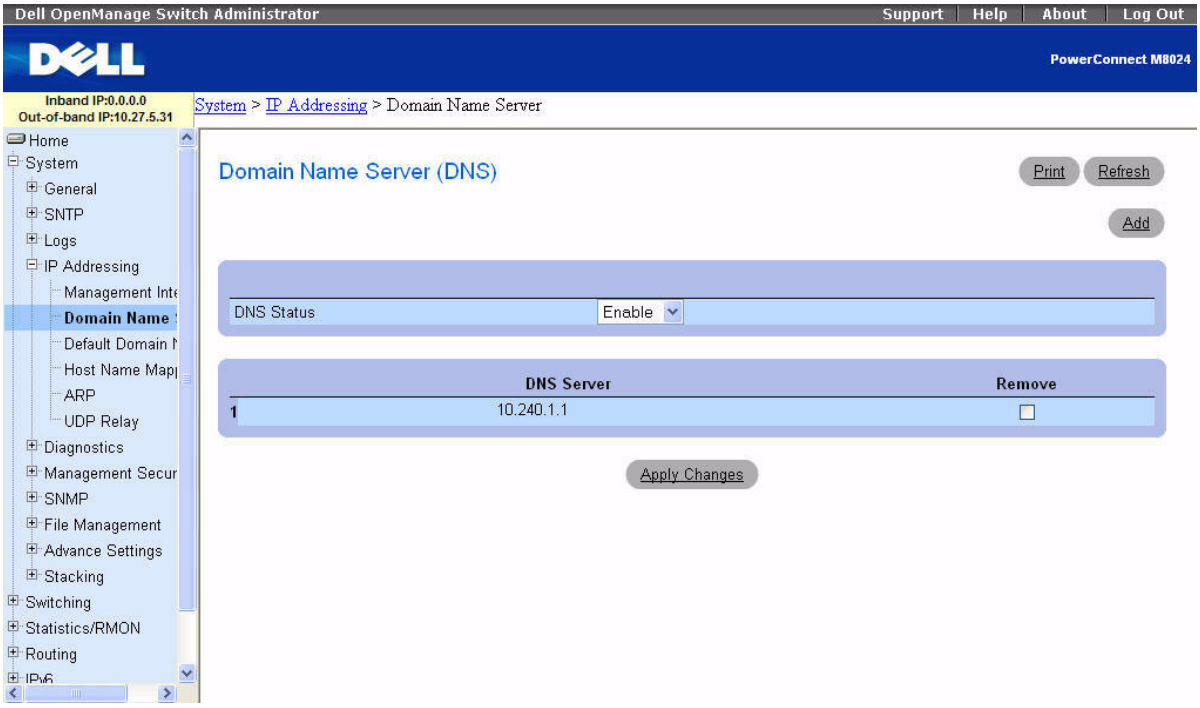
Domain Name Server (DNS)

The Domain Name System converts user-defined domain names into IP addresses. Each time a domain name is assigned, this service translates the name into a numeric IP address. For example, **www.ipexample.com** is translated to 192.87.56.2. Domain Name System servers maintain domain name databases and their corresponding IP addresses.

Use the **Domain Name Server (DNS)** page to enable and activate specific DNS servers.

To display the **Domain Name Server** page, click **System > IP Addressing > Domain Name Server** in the tree view.

Figure 6-25. Domain Name Server



The **Domain Name Server (DNS)** page contains the following fields:

- **DNS Status** — Enables or disables translating DNS names into IP addresses.
- **DNS Server** — Contains a list of DNS servers. DNS servers are added in the **Add DNS Server** page.
- **Remove** — When selected, removes the selected DNS server.

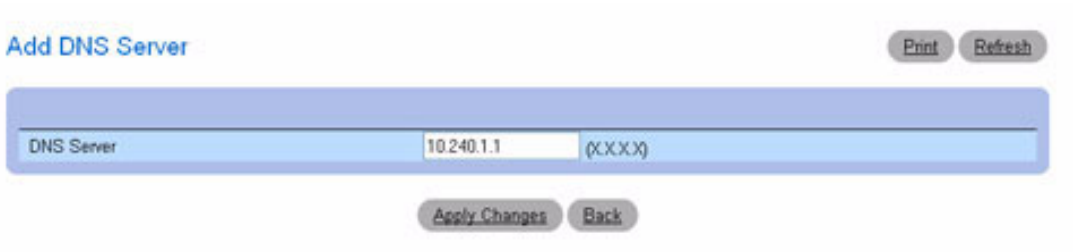
Downloaded from www.Manualslib.com manuals search engine

Adding a DNS Server

1. Open the **Domain Name Server (DNS)** page.
2. Click **Add**.

   The **Add DNS Server** page displays:

Figure 6-26. Add DNS Server



3. Define the relevant fields.
4. Click **Apply Changes**.

   The new DNS server is defined, and the device is updated.

Configuring DNS Servers Using the CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- IP Addressing Commands.

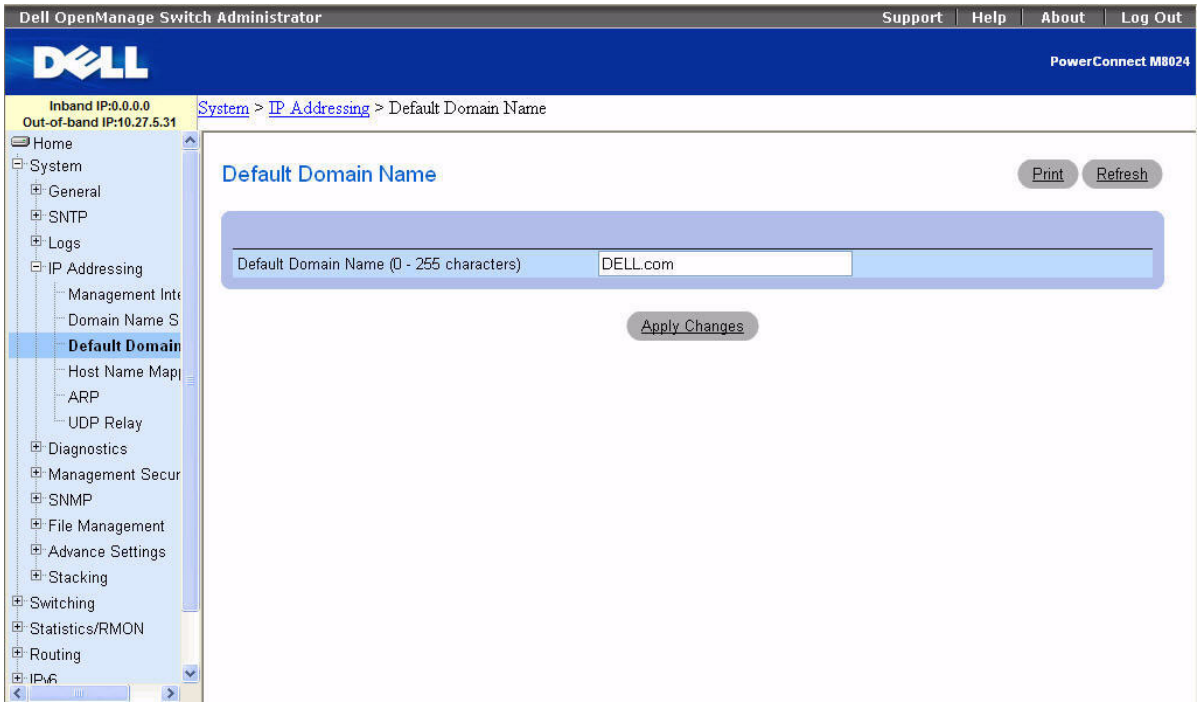
Default Domain Name

Use the **Default Domain Name** page to view and define default DNS domain names.

To display the **Default Domain Name** page, click **System > IP Addressing > Default Domain Name**.

Downloaded from www.Manualslib.com manuals search engine

Figure 6-27. Default Domain Name



The **Default Domain Name** page contains the following field:

- **Default Domain Name (0–255 characters) —** Contains the user-defined default domain name. When configured, the default domain name is applied to all unqualified host names.

Defining DNS Domain Names Using the CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- IP Addressing Commands.

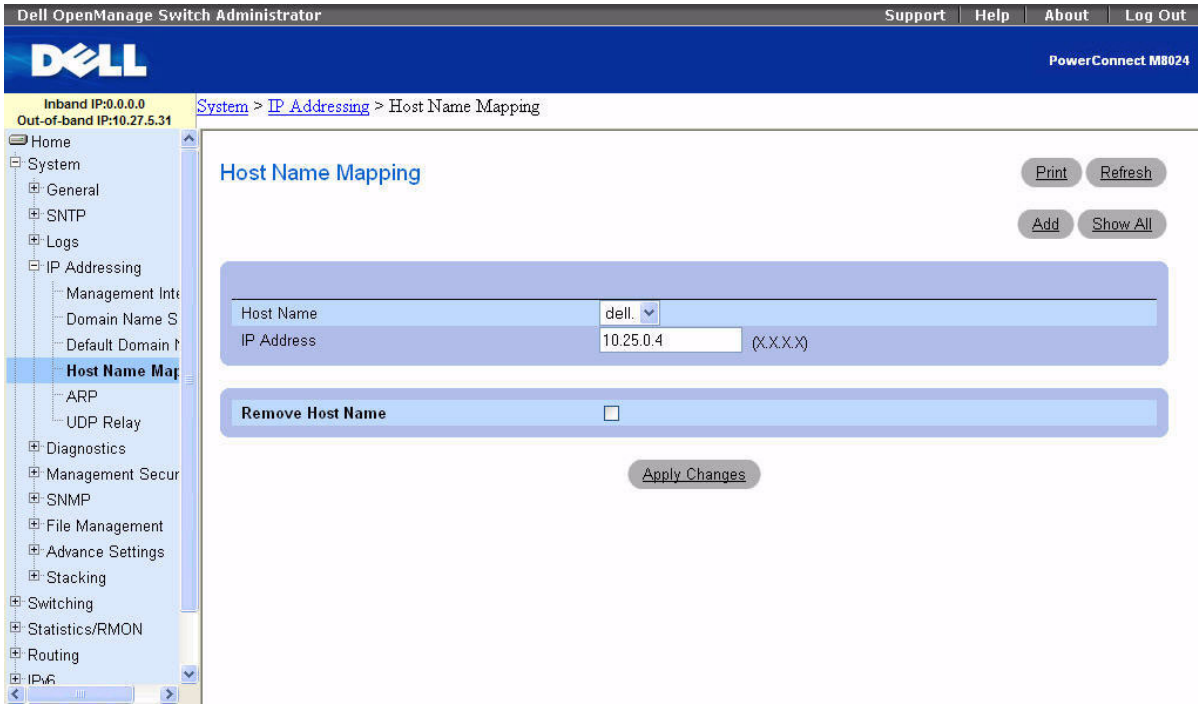
Downloaded from www.Manualslib.com manuals search engine

Host Name Mapping

Use the **Host Name Mapping** page to assign an IP address to a static host name. The **Host Name Mapping** page provides one IP address per host.

To display the **Host Name Mapping** page, click **System > IP Addressing > Host Name Mapping.**

Figure 6-28. Host Name Mapping



The **Host Name Mapping** page contains the following fields:

- **Host Name —** Contains a list of host names. Host names are defined on the **Add Static Host Name Mapping** page. Each host provides one IP address.
- **IP Address —** Provides an IP address that is assigned to the specified host name.
- **Remove Host Name —** Removes the host name IP mapping when checked.

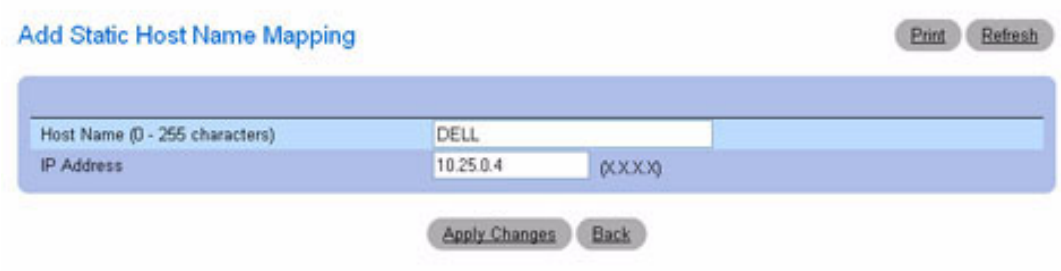
Adding Host Domain Names

1. Open the **Host Name Mapping** page.
2. Click **Add**.

   The **Add Static Host Name Mapping** page displays:

Downloaded from www.Manualslib.com manuals search engine

Figure 6-29. Add Static Host Name Mapping



3. Define the relevant fields.
4. Click **Apply Changes**.

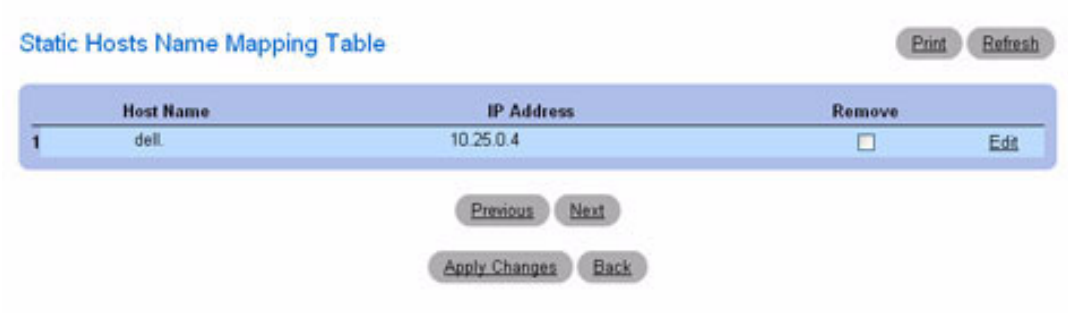
   The IP address is mapped to the host name, and the device is updated.

Displaying the Static Host Name Mapping Table

1. Open the **Host Name Mapping** page.
2. Click **Show All**.

   The **Static Host Name Mapping Table** displays:

Figure 6-30. Static Host Name Mapping Table



Removing a Host Name From IP Address Mapping

1. Open the **Host Name Mapping** page.
2. Click **Show All**.

   The **Host Name Mapping Table** opens.
3. Select a Host Name Mapping Table entry.
4. Check the **Remove** check box.
5. Click **Apply Changes**.

The Host Name Mapping Table entry is removed, and the device is updated.

Downloaded from www.Manualslib.com manuals search engine

Mapping an IP Address to Domain Host Names Using the CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

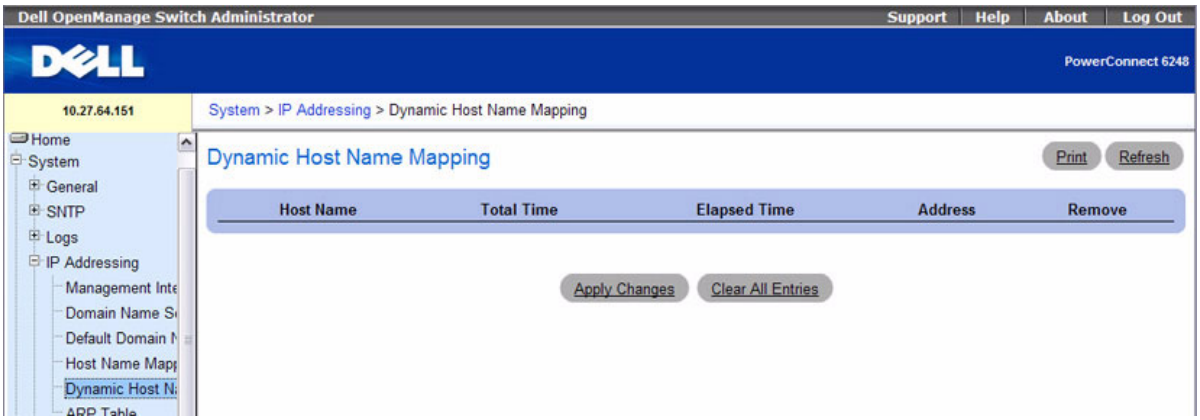
- IP Addressing Commands.

Dynamic Host Name Mapping

Use the **Dynamic Host Name Mapping** page to view dynamic host entries the switch has learned.

To display the **Dynamic Host Name Mapping** page, click **System** > **IP Addressing** > **Dynamic Host Name Mapping** in the tree view.

Figure 6-31. Dynamic Host Name Mapping



The **Dynamic Host Name Mapping** page contains the following fields:

- **Host Name** — Contains a list of host names.
- **Total Time** — Total time of the dynamic entry.
- **Elapsed Time** — Elapsed time of the dynamic entry.
- **Address** — IP address of dynamic entry.
- **Remove** — Select the entry to remove from the table, and then click **Apply Changes** to remove the selected entry from the Host Name IP Mapping list.

Click **Clear All Entries** to remove all Host Name IP Mapping entries from the table.

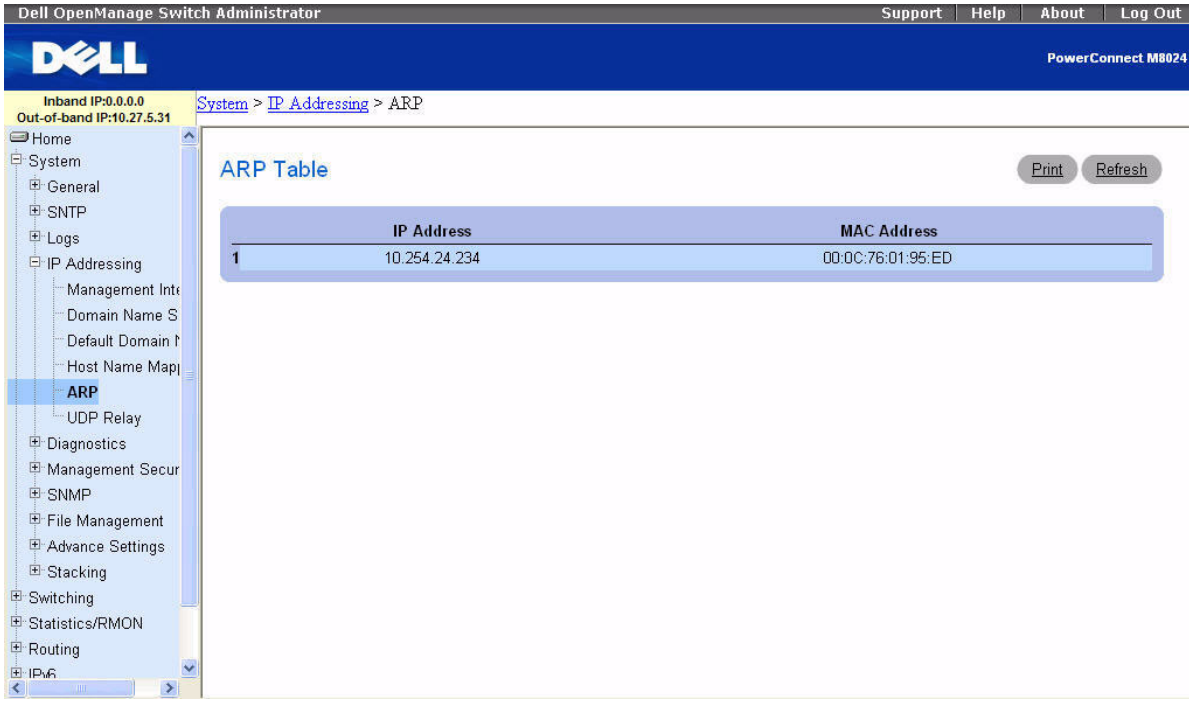
Downloaded from www.Manualslib.com manuals search engine

ARP Table

Use the **ARP Table** page to view ARP parameters for IP interfaces. The ARP table displays the correlation between each MAC address and its corresponding IP address.

To display the **ARP Table** page, click **System** > **IP Addressing** > **ARP** in the tree view.

Figure 6-32. ARP Table



The **ARP Table** page contains the following fields:

- **IP Address** — The station IP address, which is associated with the MAC address filled in below.
- **MAC Address** — The station MAC address, which is associated in the ARP table with the IP address.

Viewing the ARP Table Using the CLI Command

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- IP Addressing Commands.

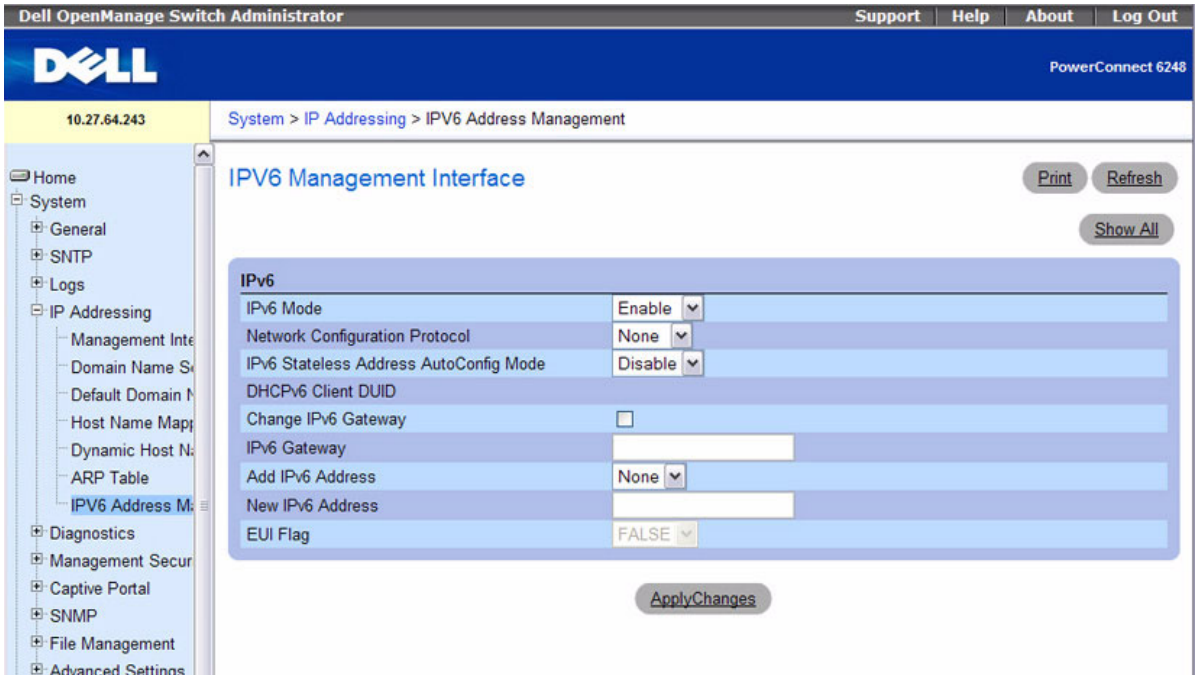
Downloaded from www.Manualslib.com manuals search engine

IPv6 Management Features

The PowerConnect M6220/M6348/M8024 switch software includes several enhancements to the IPv6 management feature. You can assign either an IPv4 or IPv6 address to the management interface. In previous software releases, the management port supported IPv6 addresses, but only when the switch received its IPv6 addressing and gateway definitions through auto-configuration when connected to an IPv6 router on the management network. Support for host name mapping to a host with an IPv6 address is also present.

To display the **IPv6 Management Interface** page, click **System > IP Addressing > IPv6 Address Management** in the tree view.

Figure 6-33. IPv6 Address Management



The **IPv6 Address Management** page contains the following fields:

- **IPv6 Mode** —Enables or disables IPv6 mode on the management interface.
- **Network Configuration Protocol** — Specify whether to use DHCP for dynamic IPv6 address assignment. If you select None, you can configure a static IPv6 address.
- **IPv6 Stateless Address AutoConfig Mode** — Enable or disable IPv6 auto address configuration on the interface. When IPv6 AutoConfig Mode is enabled, automatic IPv6 address configuration and gateway configuration is allowed by processing the Router Advertisements received on the management interface.
- **DHCPv6 Client DUID** — This is a read-only field that contains a unique ID generated from the MAC address when the DHCPv6 client is enabled. To get the value for this field, set the network protocol to DHCP.

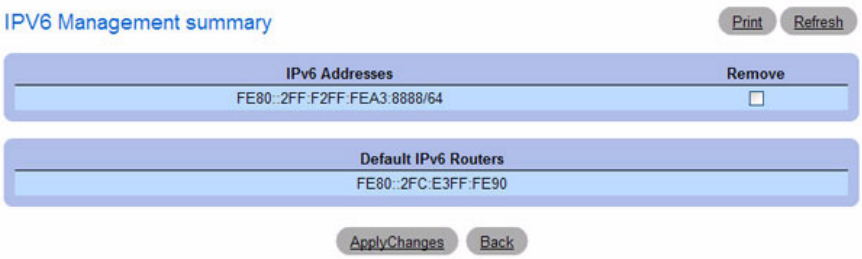
Downloaded from www.Manualslib.com manuals search engine

- **Change IPv6 Gateway** — Select this option to allow the IPv6 Gateway field to be edited.
- **IPv6 Gateway** — Enter the IPv6 gateway address (do not include a prefix). Use an IPv6 global or link-local address format.
- **Add IPv6 Address** — To add an IPv6 address, select Add so you can specify an address in the New IPv6 Address field.
- **New IPv6 Address** — If **Add** is selected from the Add IPv6 Address field, enter an IPv6 prefix/length in this field.
- **EUI Flag** — Select True if the last 64 bits are to be derived from the MAC address. For example, you can enter 2001::/64 and have the EUI Flag (True) use the 64-bit address calculated from the MAC address.

Displaying IPv6 Address Management Information

1. Open the **IPv6 Address Management** page.
2. Click **Show All** to display the **IPv6 Management Summary** page.

Figure 6-34. IPv6 Management Summary



3. To remove an IPv6 Address, select the Remove option associated with the address, and click **Apply Changes**.

Downloaded from www.Manualslib.com manuals search engine

Running Cable Diagnostics

Use the **Diagnostics** menu page to perform virtual cable tests for copper and fiber optics cables.

To display the **Diagnostics** page, click **System > Diagnostics** in the tree view.

Use this page to go to the following feature:

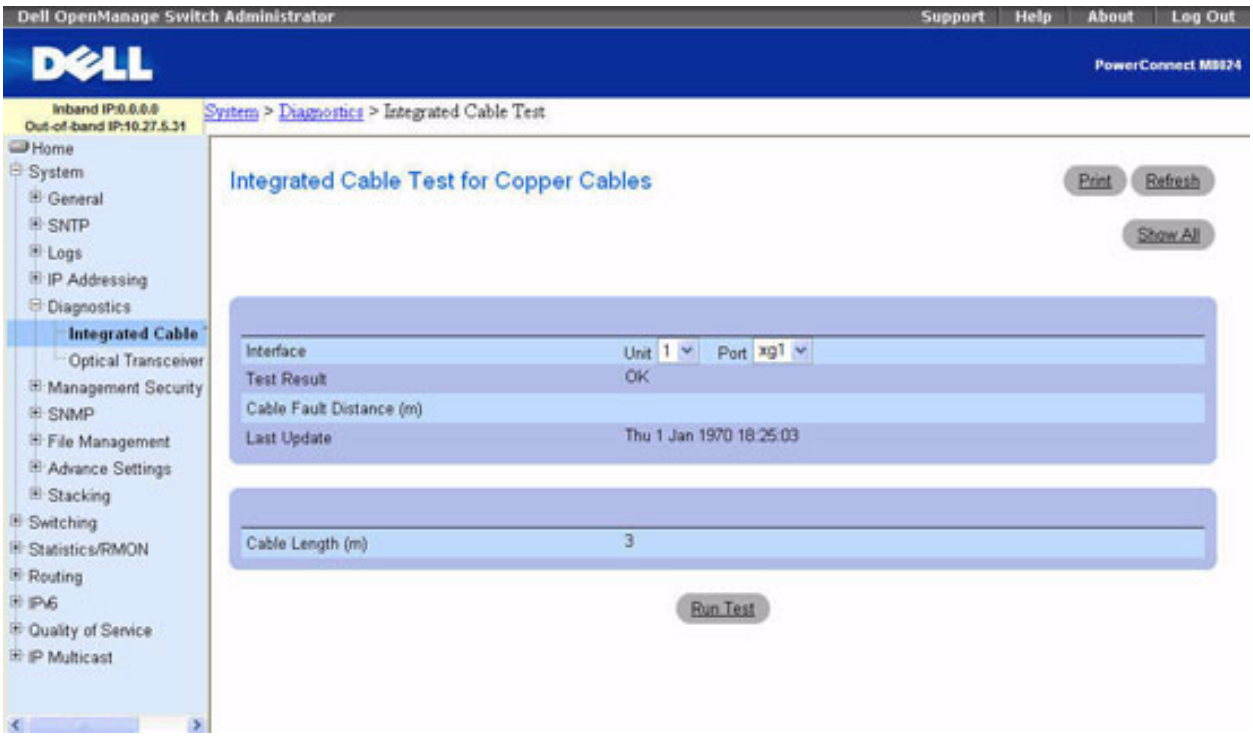
- Integrated Cable Test for Copper Cables

Integrated Cable Test for Copper Cables

Use the **Integrated Cable Test for Copper Cables** page to perform tests on copper cables. Cable testing provides information about where errors occurred in the cable, the last time a cable test was performed, and the type of cable error which occurred. The tests use Time Domain Reflectometry (TDR) technology to test the quality and characteristics of a copper cable attached to a port. Cables up to 120 meters long can be tested. Cables are tested when the ports are in the down state, with the exception of the Approximated Cable Length test.

To display the **Integrated Cable Test for Copper Cables** page, click **System > Diagnostics > Integrated Cable Test** in the tree view.

Figure 6-35. Integrated Cable Test for Copper Cables



Downloaded from www.Manualslib.com manuals search engine

The **Integrated Cable Test for Copper Cables** page contains the following fields:

- **Interface —** The interface to which the cable is connected.
- **Test Result —** The cable test results. Possible values are:
  - **No Cable** — There is not a cable connected to the port.
  - **Open Cable** — The cable is open.
  - **Short Cable** — A short has occurred in the cable.
  - **OK** — The cable passed the test.
  - **Fiber Cable** — A fiber cable is connected to the port.
- **Cable Fault Distance** — The distance from the port where the cable error occurred.
- **Last Update** — The last time the port was tested.
- **Cable Length** — The approximate cable length. This test can only be performed when the port is up and operating at 1 Gbps.

Performing a Cable Test

1. Ensure that both ends of the copper cable are connected to a device.
2. Open the **Integrated Cable Test for Copper Cables** page.
3. Click **Run Test**.

   The copper cable test is performed, and the results are displayed on the **Integrated Cable Test for Copper Cables** page.

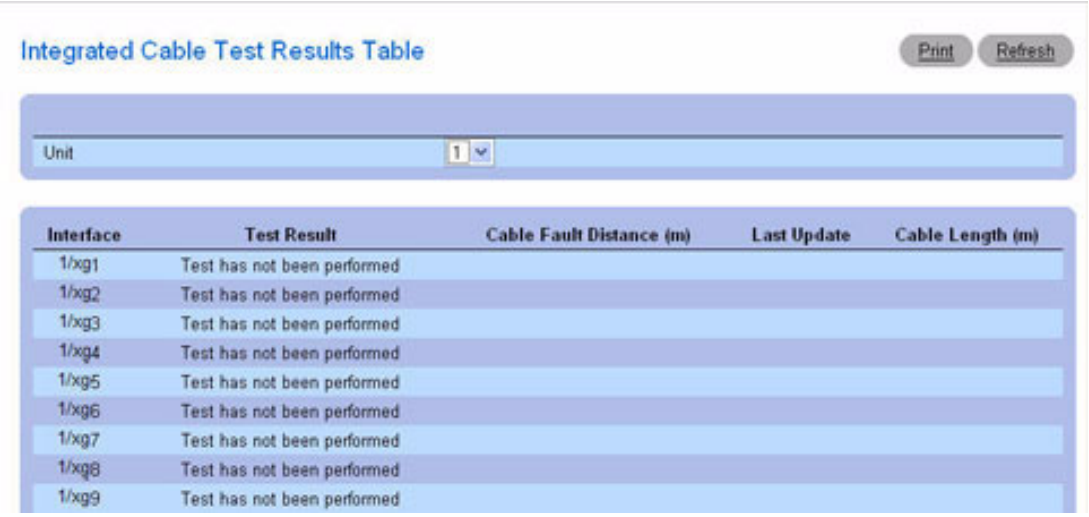
Displaying Integrated Cable Test Results Table

1. Open the **Integrated Cable Test for Copper Cables** page.
2. Click **Show All**.
3. Select the desired unit from the drop-down menu.

   The web page displays the **Integrated Cable Test Results Table** page showing the results of previous tests for every port on the selected unit.

Downloaded from www.Manualslib.com manuals search engine

Figure 6-36. Integrated Cable Test Results Table



Performing Copper Cable Tests Using CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- PHY Diagnostics Commands.

Optical Transceiver Diagnostics

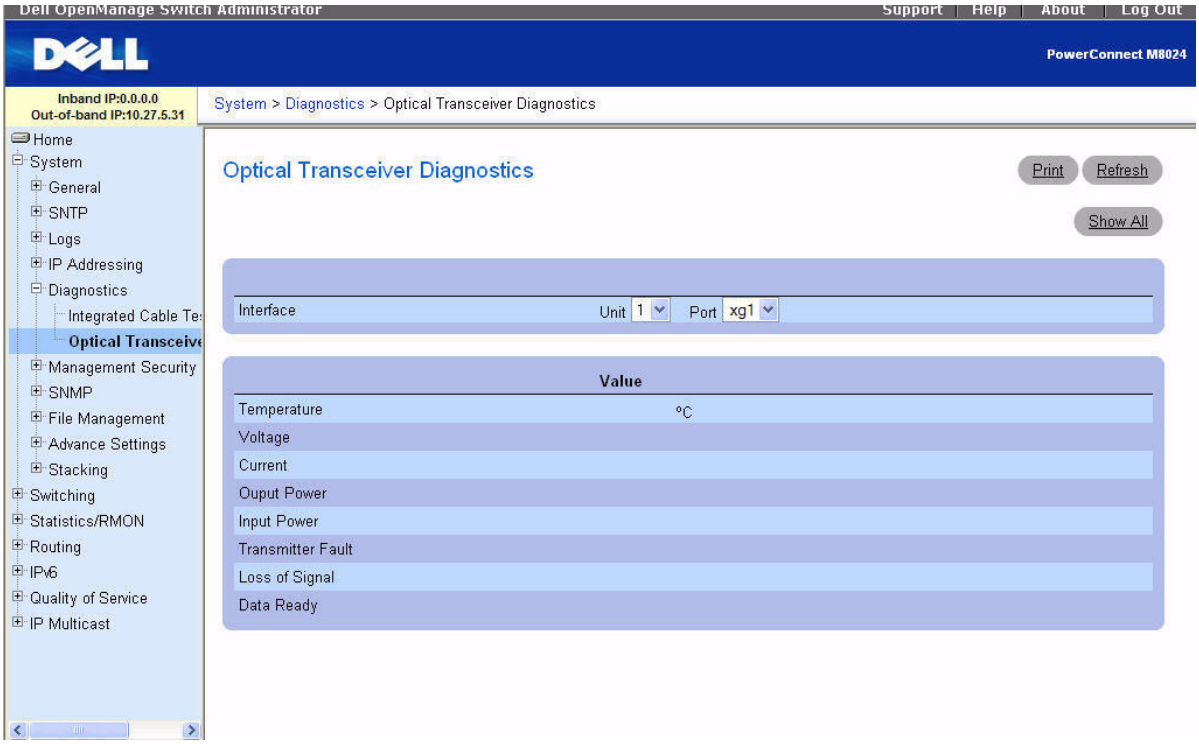
Use the **Optical Transceiver Diagnostics** page to perform tests on Fiber Optic cables.

To display the **Optical Transceiver Diagnostics** page, click **System > Diagnostics > Optical Transceiver Diagnostics** in the tree view.

Note: Optical transceiver diagnostics can be performed only when the link is present.

Downloaded from www.Manualslib.com manuals search engine

Figure 6-37. Optical Transceiver Diagnostics



The **Optical Transceiver Diagnostics** page contains the following fields:

- **Interface** — The port IP address on which the cable is tested.
- **Temperature** — The temperature (C) at which the cable is operating.
- **Voltage** — The voltage at which the cable is operating.
- **Current** — The current at which the cable is operating.
- **Output Power —** The rate at which the output power is transmitted.
- **Input Power** — The rate at which the input power is transmitted.
- **Transmitter Fault —** Indicates if a fault occurred during transmission.
- **Loss of Signal** — Indicates if a signal loss occurred in the cable.
- **Data Ready** — Indicates the transceiver has achieved power up and data is ready.

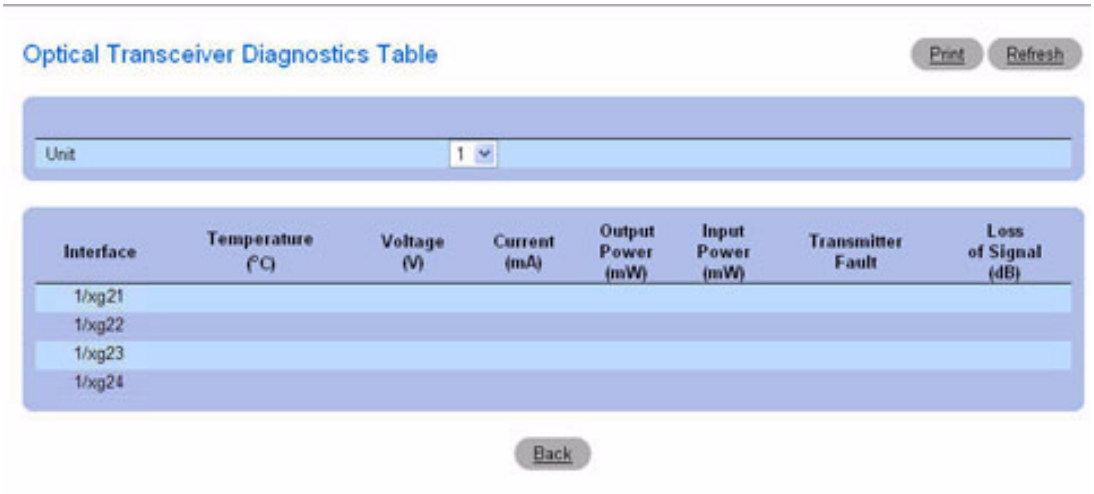
Note: Finisar transceivers do not support the transmitter fault diagnostic testing. Fiber Optic analysis feature works only on SFPs that support the digital diagnostic standard SFF-4872.

Displaying Optical Transceiver Diagnostics Test Results Table

1. Open the **Optical Transceiver Diagnostics** page.
2. Click **Show All**.
3. Select the desired unit from the drop-down menu.

Downloaded from www.Manualslib.com manuals search engine

Figure 6-38. Optical Transceiver Diagnostics Table



The test runs and displays the Optical Transceiver Diagnostics Table page.

Performing Fiber Optic Cable Tests Using CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- PHY Diagnostics Commands.

Managing Device Security

Use the **Management Security** menu page to set management security parameters for port, user, and server security.

To display the **Management Security** page, click **System > Management Security** in the tree view. Use this page to go to the following features:

- Access Profile
- Authentication Profiles
- Select Authentication
- Password Management
- Local User Database
- Line Passwords
- Enable Password
- TACACS+ Settings
- RADIUS Global Configuration
- RADIUS Server Configuration

Downloaded from www.Manualslib.com manuals search engine

- RADIUS Accounting Server Statistics
- RADIUS Server Statistics
- Authorization Network RADIUS
- Telnet Server
- Denial of Service

Access Profile

Use the **Access Profile** page to define a profile and rules for accessing the device. You can limit access to specific management functions, to specific ingress interfaces, and/or to source IP address and/or source IP subnets. The feature has been modified to include TFTP in the list of management access methods.

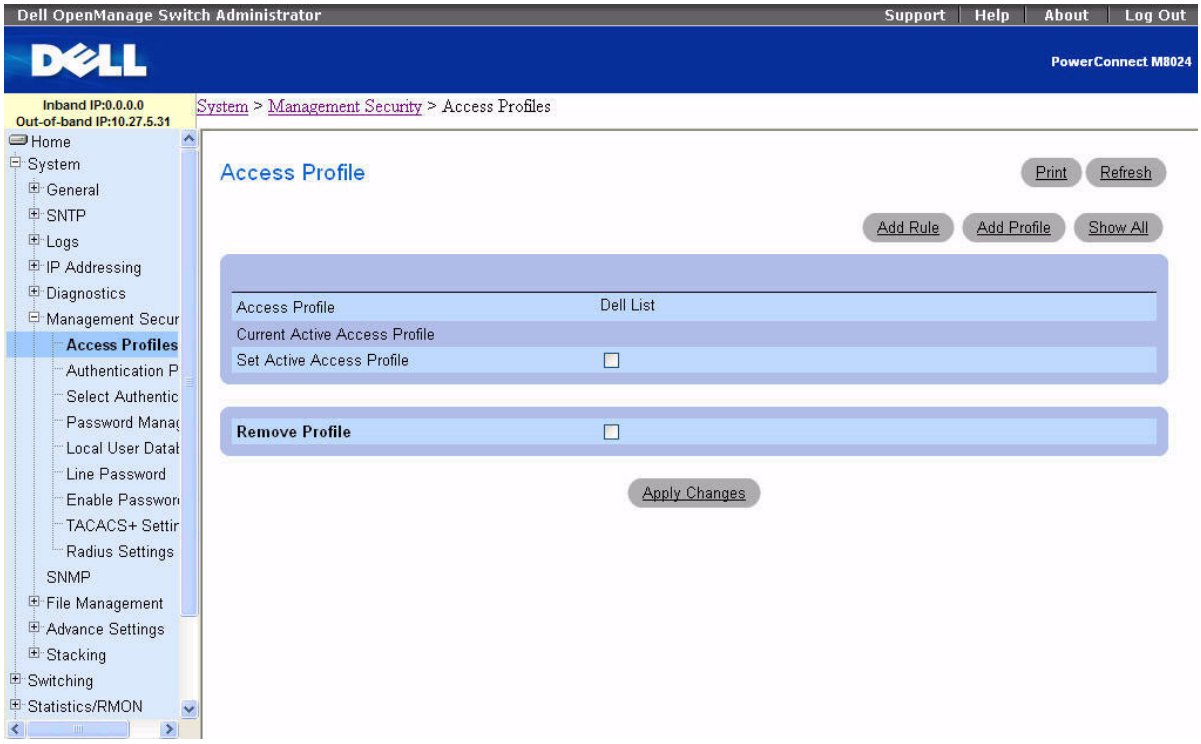
Management access can be separately defined for each type of management access method, including, Web (HTTP), Secure web (HTTPS), Telnet, SSH, TFTP, and SNTP.

To display the **Access Profile** page, click **System** > **Management Security** > **Access Profiles** in the tree view.

When you add a profile or a rule from the **Access Profile** page, the Management Method field on the **Add Profile** and **Add Rule** pages now contains the TFTP option. Select the TFTP option to limit the user's access method to TFTP.

Downloaded from www.Manualslib.com manuals search engine

Figure 6-39. Access Profile



- **Access Profile** — Shows the Access Profile.
- **Current Active Access Profile** — Shows profile that is activated.
- **Set Active Access Profile** — Activates the access profile.
- **Remove Profile** — When checked, removes an access profile from the **Access Profile** list.

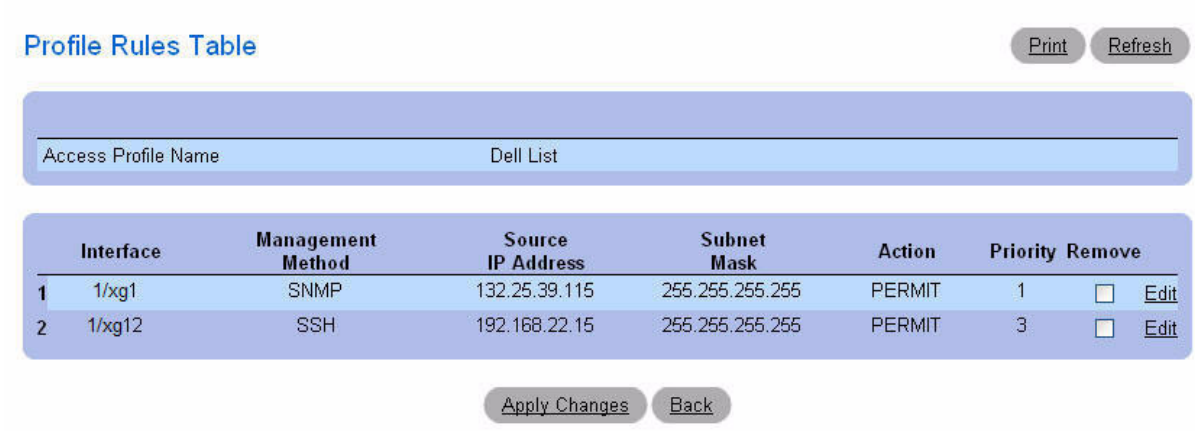
Note: Assigning an access profile to an interface implies that access through other interfaces is denied. If an access profile is not activated, the device can be accessed by all.

Displaying the Access Profile

1. Open the **Access Profile** page.
2. Click **Show All** to display the **Profile Rules Table** page.

Downloaded from www.Manualslib.com manuals search engine

Figure 6-40. Profile Rules Table

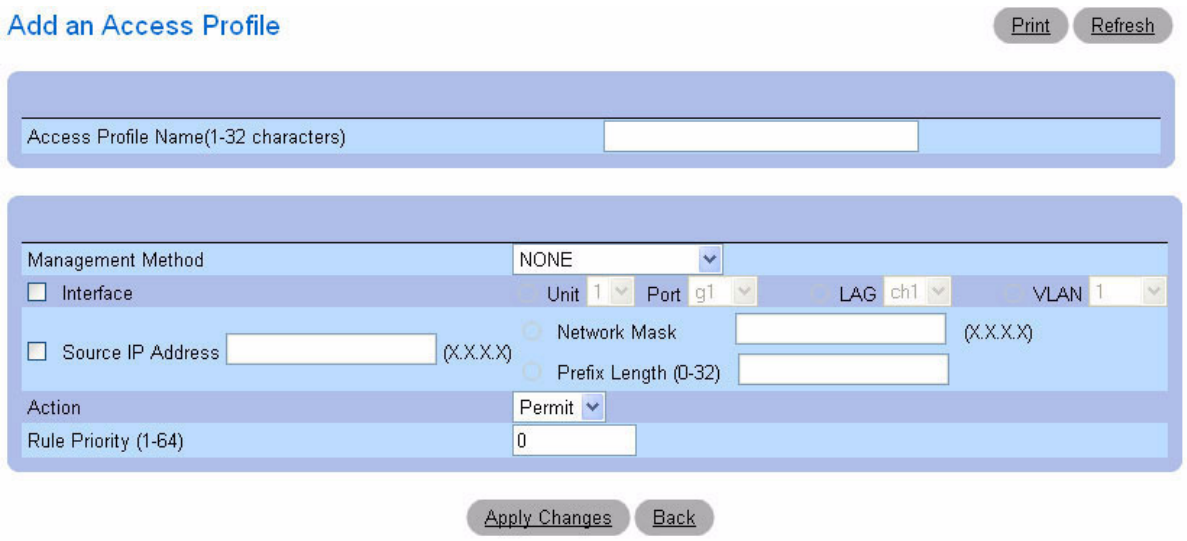


Adding an Access Profile

1. Open the **Access Profile** page.
2. Click **Add Profile**.

   The **Add an Access Profile** page displays.

Figure 6-41. Add an Access Profile



3. Enter the profile name in the **Access Profile Name** text box.
4. Complete the fields:

Downloaded from www.Manualslib.com manuals search engine

Management Method — Select from the dropdown box. The policy is restricted by the management chosen.

Interface — Choose the check box for the interface if the policy should have a rule based on the interface. Interface can be a physical interface, a LAG, or a VLAN.

Source IP Address — Select the **Source IP Address** check box if the policy should have a rule based on the IP address of the client sending the management traffic. Fill in the source IP address and mask details in the fields provided. Note that Mask can be given in two formats: either dotted IP format (for example, 255.255.255.0) or prefix length (for example, 32)

Action — Choose the action to be performed when the rules selected above are matched. Use the dropdown box and choose Permit or Deny to permit or deny access.

Rule Priority — Configure priorities to the rules. The rules are validated against the incoming management request in the ascending order of their priorities. If a rule matches, action is performed and rules below are ignored. For example, if you configure Source IP 10.10.10.10 with priority 1 to Permit, and configure Source IP 10.10.10.10 with priority 2 to Deny, then access is permitted if the profile is active, and the second rule is ignored.

5. Click **Apply Changes**.

   The new access profile is added, and the device is updated.

Activating an Access Profile

1. Open the **Access Profile** page.
2. Check **Set Access Profile Active**.
3. Click **Apply Changes**.

   The access profile is enabled for the device.

Adding Rules to an Access Profile

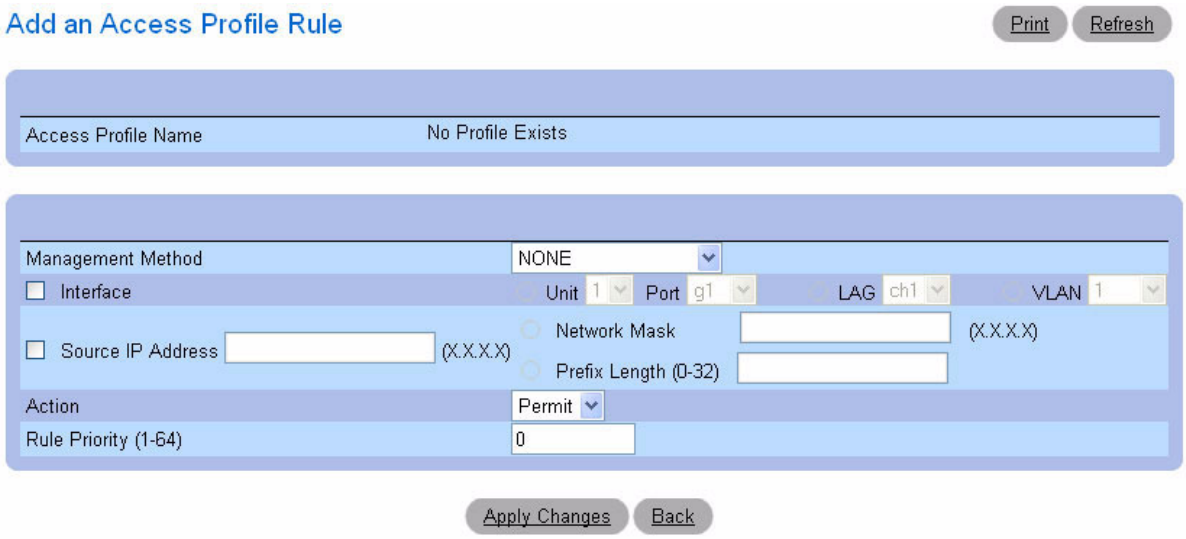
1. Open the **Access Profile** page.

   The **Access Profile** field shows the profile to which rules are added when the **Add An Access Profile Rule** page is displayed.
2. Click **Add Rule**.

   The **Add An Access Profile Rule** page displays.

Downloaded from www.Manualslib.com manuals search engine

Figure 6-42. Add An Access Profile Rule



3. Complete the fields in the dialog:

   Management Method — Select from the dropdown box. The policy is restricted by the management chosen.

   Interface — Choose the check box for the interface if the policy should have a rule based on the interface. Interface can be a physical interface, a LAG, or a VLAN.

   Source IP — Select the **Source IP Address** check box if the policy should have a rule based on the IP address of the client originating the management traffic. Fill in the source IP address and Mask details in the text boxes provided. Note that Mask can be given in two formats - either dotted IP format (for example, 255.255.255.0) or prefix length (for example, 32)

   Action — Choose the action to be performed when the rules selected above are matched. Use the dropdown box and choose Permit or Deny to permit or deny access.

   Rule Priority — Configure priorities to the rules. The rules are validated against the incoming management request in the ascending order of their priorities. If a rule matches, action is performed and rules below are ignored. For example, if you configure Source IP 10.10.10.10 with priority 1 to Permit, and configure Source IP 10.10.10.10 with priority 2 to Deny, then access is permitted if the profile is active, and the second rule is ignored.

4. Click **Apply Changes**.

   The rule is added to the access profile, and the device is updated.

Downloaded from www.Manualslib.com manuals search engine

Removing a Rule

1. Open the **Access Profile** page.
2. Click **Show All** to display the **Profile Rules Table** page.
3. Select a rule.
4. Check the **Remove** check box.
5. Click **Apply Changes**.

   The rule is removed, and the device is updated.

Defining Access Profiles Using CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- Management ACL Commands.

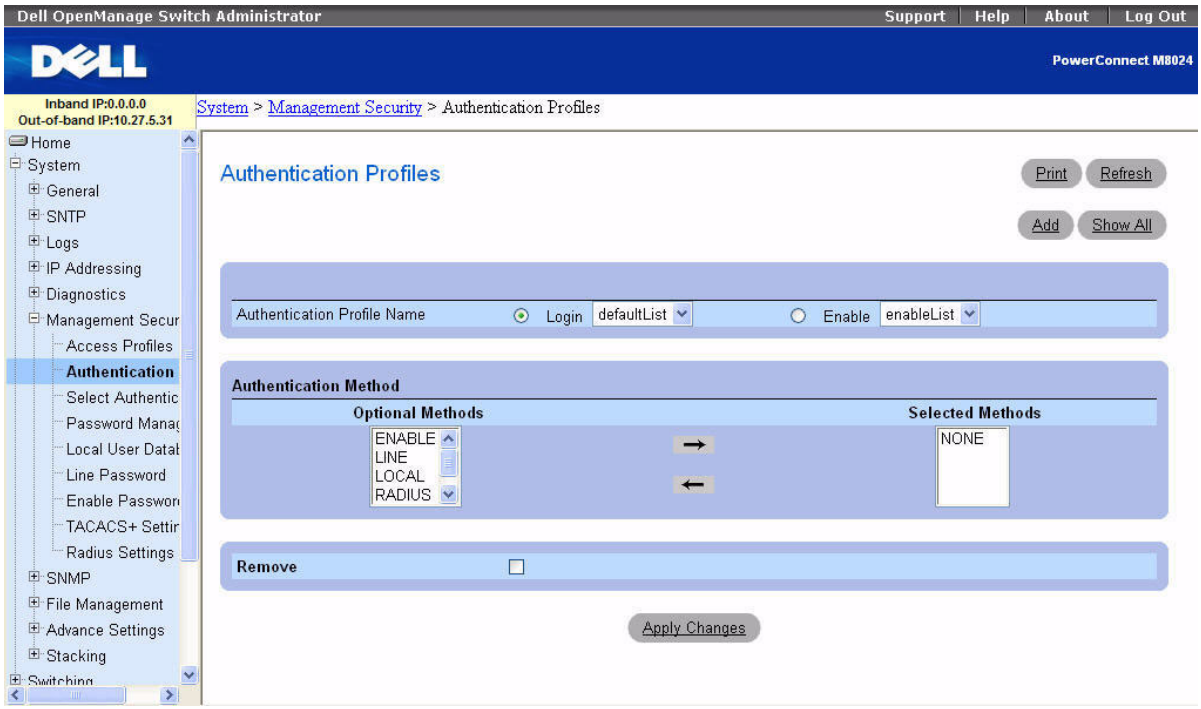
Authentication Profiles

User authentication occurs locally and on an external server. Use the **Authentication Profiles** page to select the user authentication method on the device.

To display the **Authentication Profiles** page, click **System** > **Management Security** > **Authentication Profiles** in the tree view.

Downloaded from www.Manualslib.com manuals search engine

Figure 6-43. Authentication Profiles



The **Authentication Profiles** page contains the following fields:

Authentication Profile Name

Displays lists to which user-defined authentication profiles are added. Use the radio buttons to apply the authentication profile to govern either Login or Enable part of the switch's operations, and to select one of two available lists:

- **Login** — Allows you to login to the switch. Options are **defaultList**, **networkList** and any user-defined login authentication profiles.
- **Enable** — Enables privilege mode.

Downloaded from www.Manualslib.com manuals search engine

Authentication Method

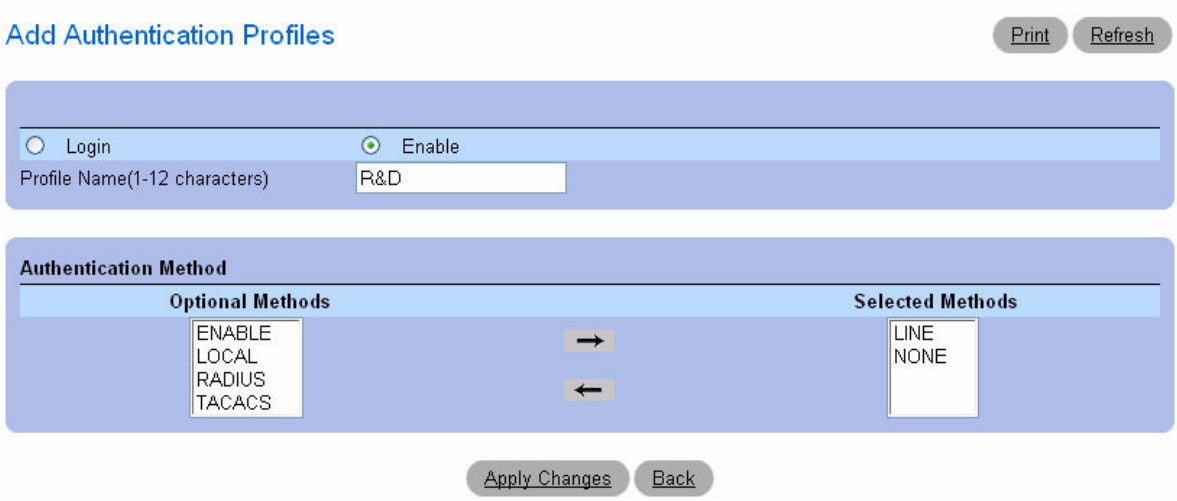
- **Optional Methods** — User authentication methods. Possible options are:
  - **None** — No user authentication occurs.
  - **Local** — User authentication occurs at the device level; the device checks the user name and password for authentication.
  - **RADIUS** — User authentication occurs at the RADIUS server. For more information about RADIUS servers, see "RADIUS Global Configuration."
  - **TACACS+** — User authentication occurs at the TACACS+ server. For more information about TACACS+ servers, see "TACACS+ Settings."
  - **Line** — The line password is used for user authentication.
  - **Enable** — The enable password is used for authentication.

  Note: User authentication occurs in the order the methods are selected. If an error occurs during the authentication, the next selected method is used. For example, if **Local** then **RADIUS** options are selected, the user is authenticated first locally and then through an external **RADIUS** server.
- **Selected Methods** — The selected authentication method.
- **Remove** — Removes the selected profile.

Adding an Authentication Profile

1. Open the **Authentication Profiles** page.
2. Click **Add** to display the **Add Authentication Profile** page.

Figure 6-44. Add Authentication Profile



Downloaded from www.Manualslib.com manuals search engine

3. Enter the profile name of 1 to 12 characters in the **Profile Name** field.

   Note: The profile name should not include spaces.

4. Click **Apply Changes**.

   A profile is created. You can activate an authentication profile using the **System** > **Management Security** > **Select Authentication** web page.

Modifying Authentication Profiles

1. Open the **Authentication Profiles** page.
2. Select an element from the list in the **Authentication Profile Name** field.
3. Select one or more **Optional Methods** by using the arrows.
4. Click **Apply Changes**.

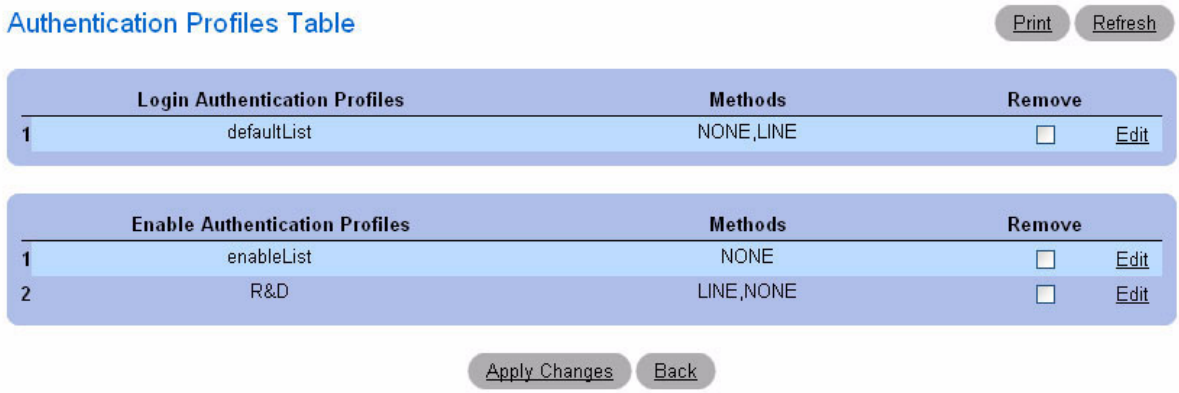
   The user authentication profile is updated to the device.

Removing an Authentication Profiles Entry

1. Open the **Authentication Profiles** page.
2. Click **Show All**.

   The **Authentication Profiles** Table opens.

Figure 6-45. Authentication Profiles Table



3. Check the **Remove** check box next to the profile to be removed.
4. Click **Apply Changes**.

   The entry is removed.

Downloaded from www.Manualslib.com manuals search engine

Configuring an Authentication Profile Using CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

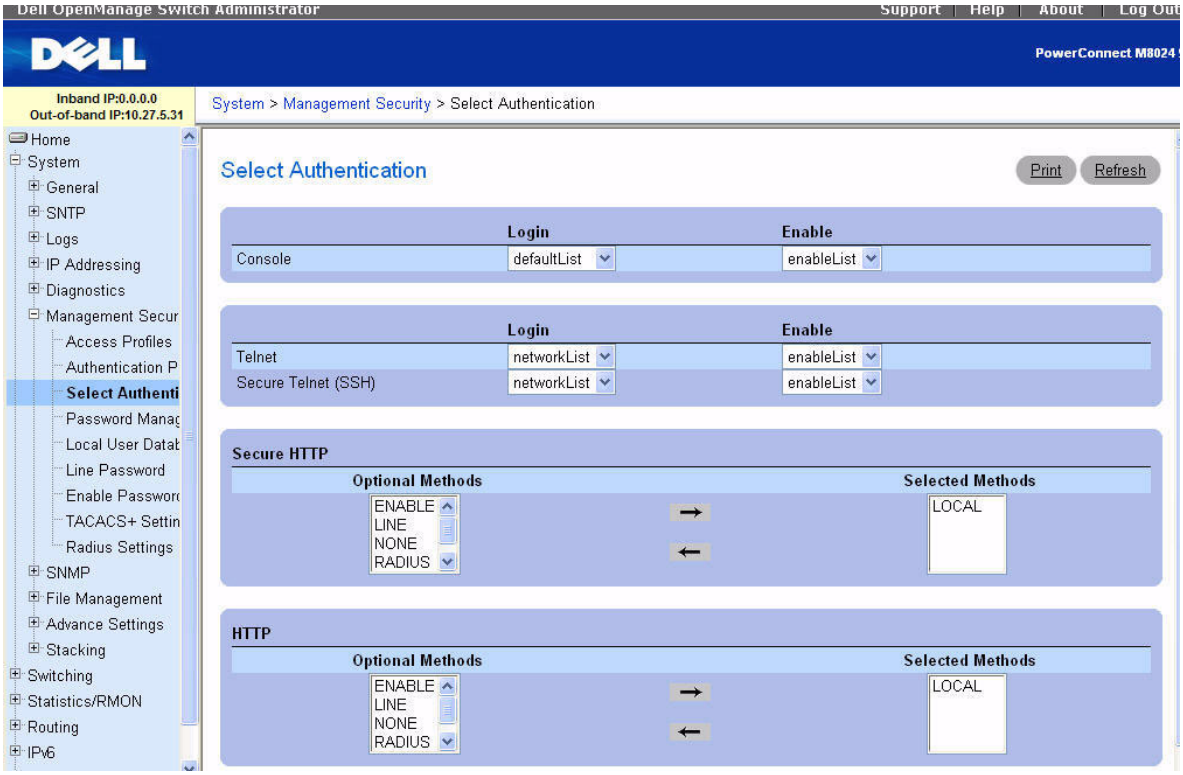
- AAA Commands.

Select Authentication

After authentication profiles are defined, you can apply them to management access methods. For example, console users can be authenticated by Authentication Profile List 1, while Telnet users are authenticated by Authentication Profile List 2.

To display the **Select Authentication** page, click **System > Management Security > Select Authentication** in the tree view.

Figure 6-46. Select Authentication



The **Select Authentication** page contains the following fields:

- **Console** — Authentication profiles used to authenticate console users.
- **Telnet** — Authentication profiles used to authenticate Telnet users.
- **Secure Telnet (SSH)** — Authentication profiles used to authenticate Secure Shell (SSH) users. SSH provides clients secure and encrypted remote connections to a device.

Downloaded from www.Manualslib.com manuals search engine

- **Secure HTTP and HTTP** — Authentication method used for Secure HTTP access and HTTP access, respectively. Possible field values are:
  - **None** — No authentication method is used for access.
  - **Local** — Authentication occurs locally.
  - **RADIUS** — Authentication occurs at the RADIUS server.
  - **TACACS+** — Authentication occurs at the TACACS+ server.
  - **Local, None** — Authentication first occurs locally.
  - **RADIUS, None** — Authentication first occurs at the RADIUS server. If authentication cannot be verified, no authentication method is used. Authentication cannot be verified if the remote server cannot be contacted to verify the user. If the remote server can be contacted, then the response from the remote server is always honored.
  - **TACACS+, None** — Authentication first occurs at the TACACS+ server. If authentication cannot be verified, no authentication method is used. Authentication cannot be verified if the remote server cannot be contacted to verify the user. If the remote server can be contacted, then the response from the remote server is always honored.
  - **Local, RADIUS** — Authentication first occurs locally. If authentication cannot be verified locally, the RADIUS server authenticates the management method. If the RADIUS server cannot authenticate the management method, the session is blocked.
  - **Local, TACACS+** — Authentication first occurs locally. If authentication cannot be verified locally, the TACACS+ server authenticates the management method. If the TACACS+ server cannot authenticate the management method, the session is blocked.
  - **RADIUS, Local** — Authentication first occurs at the RADIUS server. If authentication cannot be verified at the RADIUS server, the session is authenticated locally. If the session cannot be authenticated locally, the session is blocked.
  - **TACACS+, Local** — Authentication first occurs at the TACACS+ server. If authentication cannot be verified at the TACACS+ server, the session is authenticated locally. If the session cannot be authenticated locally, the session is blocked.
  - **Local, RADIUS, None —** Authentication first occurs locally. If authentication cannot be verified locally, the RADIUS server authenticates the management method. If the RADIUS server cannot authenticate the management method, the session is permitted.
  - **RADIUS, Local, None —** Authentication first occurs at the RADIUS server. If authentication cannot be verified at the RADIUS server, the session is authenticated locally. If the session cannot be authenticated locally, the session is permitted.
  - **Local, TACACS+, None —** Authentication first occurs locally. If authentication cannot be verified locally, the TACACS+ server authenticates the management method. If the TACACS+ server cannot authenticate the management method, the session is permitted.

Downloaded from www.Manualslib.com manuals search engine

– **TACACS+, Local, None —** Authentication first occurs at the TACACS+ server. If authentication cannot be verified at the TACACS+ server, the session is authenticated locally. If the session cannot be authenticated locally, the session is permitted.

Applying an Authentication Method List to Console Sessions

1. Open the **Select Authentication** page.
2. Select an authentication profile in the **Console** field.
3. Click **Apply Changes**.

   Console sessions are assigned an authentication method List.

Downloaded from www.Manualslib.com manuals search engine

Applying an Authentication Profile to Telnet Sessions

1. Open the **Select Authentication** page.
2. Select an authentication profile in the **Telnet** field.
3. Click **Apply Changes**.

   Console sessions are assigned authentication profiles.

Applying an Authentication Profile to Secure Telnet (SSH) Sessions

1. Open the **Select Authentication** page.
2. Select an authentication profile in the **Secure Telnet (SSH)** field.
3. Click **Apply Changes**.

   Secure Telnet (SSH) sessions are assigned authentication profiles.

Assigning HTTP Sessions an Authentication Sequence

1. Open the **Select Authentication** page.
2. Under **HTTP**, select an authentication method in the **Optional Methods** field and click the right arrow button.

   The selected authentication method moves to the **Selected Methods** field.
3. Repeat until the desired authentication sequence is displayed in the **Selected Methods** field.
4. Click **Apply Changes**.

   HTTP sessions are assigned the authentication sequence.

Assigning Access Methods, Authentication Profiles, or Sequences Using CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- AAA Commands.

Assigning Secure HTTP Sessions an Authentication Sequence

1. Open the **Select Authentication** page.
2. Under **Secure HTTP**, select an authentication method in the **Optional Methods** field and click the right arrow button.

   The selected authentication method moves to the **Selected Methods** field.
3. Repeat until the desired authentication sequence is displayed in the **Selected Methods** field.
4. Click **Apply Changes**.

   Secure HTTP sessions are assigned the authentication sequence.

Downloaded from www.Manualslib.com manuals search engine

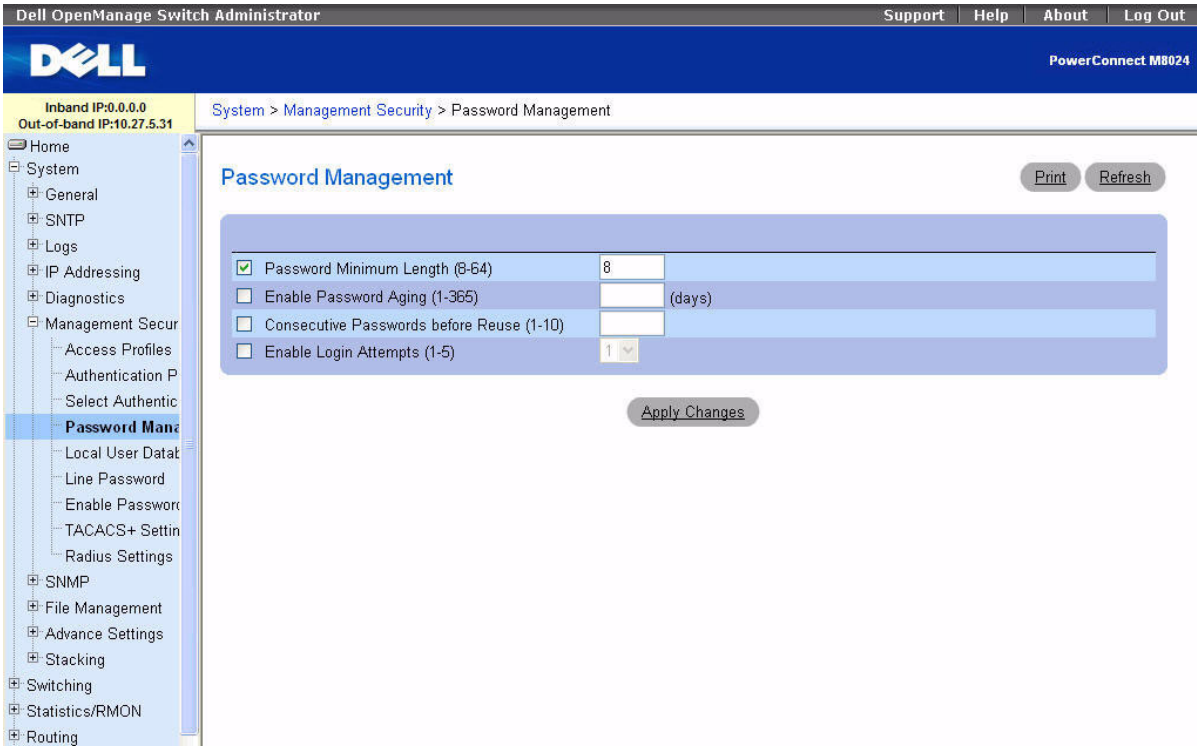
Password Management

Password management provides increased network security and improved password control. Passwords for SSH, Telnet, HTTP, HTTPS, and SNMP access are assigned security features, including:

- Defining minimum password lengths (the minimum password length is 8 when password length-checking is enabled)
- Password expiration
- Preventing frequent password reuse
- Locking out users out after failed login attempts

To display the **Password Management** page, click **System > Management Security > Password Management** in the tree view.

Figure 6-47. Password Management



The Password Management page contains the following fields:

- **Password Minimum Length** (8–64) — Indicates the minimum password length, when checked. For example, the administrator can define that all line passwords must have at least 10 characters. If you clear the check box and apply the changes, no minimum password length is required. This means that users can be created without a password.

Downloaded from www.Manualslib.com manuals search engine

- **Enable Password Aging (1–365)** — Indicates the amount of time that elapses before a password is aged out, when checked. The field value is from 1 to 365 days. The password aging feature functions only if the switch clock is synchronized to an SNTP server. See the "Clock Commands" section in the *CLI Reference Guide* for additional information.
- **Consecutive Passwords Before Reuse (1–10)** — Indicates the amount of times a password is changed, before the password can be reused. The possible field values are 1 to 10.

  Note: The user is notified to change the password prior to expiry. The Web users do not see this notification.
- **Enable Login Attempts (1–5)** — When selected, enables locking a user out of the device when a faulty password is used a defined number of times. For example, if the number of login attempts has been defined as five and the user attempts to log on five times with an incorrect password, the device locks the user out on the sixth attempt. When this happens, a super user must re-enable the user account. The field range is 1 to 5 attempts.

Defining Password Constraints

1. Open the **Password Management** page.
2. Define the relevant fields.
3. Click **Apply Changes**.

   The password constraints are defined, and the device is updated.

Defining Password Constraints Using CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- Password Management Commands.

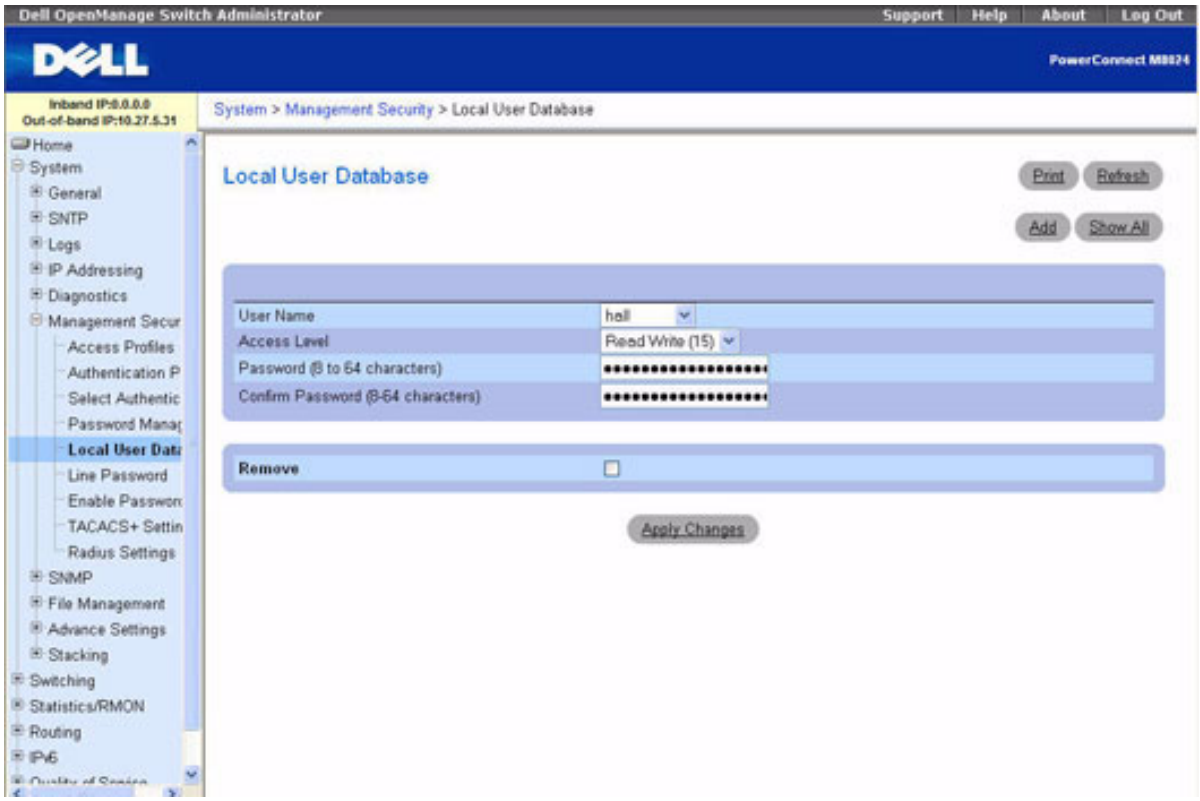
Local User Database

Use the **Local User Database** page to define passwords, access rights for users and reactivate users whose accounts have been suspended.

To display the **Local User Database** page, click **System > Management Security > Local User Database** in the tree view.

Downloaded from www.Manualslib.com manuals search engine

Figure 6-48. Local User Database



The **Local User Database** page contains the following fields:

- **User Name** — List of users.
- **Access Level** — User access level. The lowest user access level is **1** (readonly), and **15** (readwrite) is the highest. To suspend a user's access, set level to 0 (only a level 15 user has this ability).
- **Password** (8– 64 characters) — User-defined password.
- **Confirm Password —** Confirms the user-defined password.
- **Remove** — When selected, removes users from the local user database.

Assigning Access Rights to a User

1. Open the **Local User Database** page.
2. Select a user in the **User Name** field.
3. Define the fields as needed.
4. Click **Apply Changes**.

   The user's access rights and passwords are defined, and the device is updated.

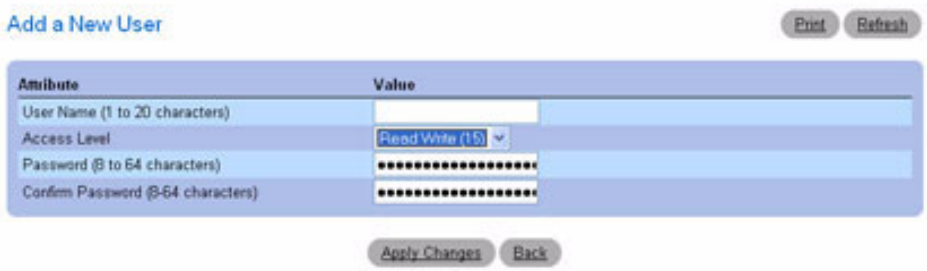
Downloaded from www.Manualslib.com manuals search engine

Adding a User to the Local User Database

1. Open the **Local User Database** page.
2. Click **Add** to display the **Add User** page.

   The **Add a New User** page is displayed.

Figure 6-49. Add a New User



3. Complete the fields.
4. Click **Apply Changes**.

   The new user is defined, and the device is updated.

Note: You can define as many as eight local users on the device.

Displaying Users on the Local User Database

1. Open the **Local User Database** page.
2. Click **Show All** to display the **Local User Table** page.

   All members of the local user database are displayed.

Figure 6-50. Local User Table

Downloaded from www.Manualslib.com manuals search engine

Removing Users From the Local User Database

1. Open the **Local User Database** page.
2. Click **Show All** to display the **Local User Table** page.
3. Select a **User Name**.
4. Check **Remove**.
5. Click **Apply Changes**.

   The user is removed, and the device is updated.

Assigning Users With CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- AAA Commands.

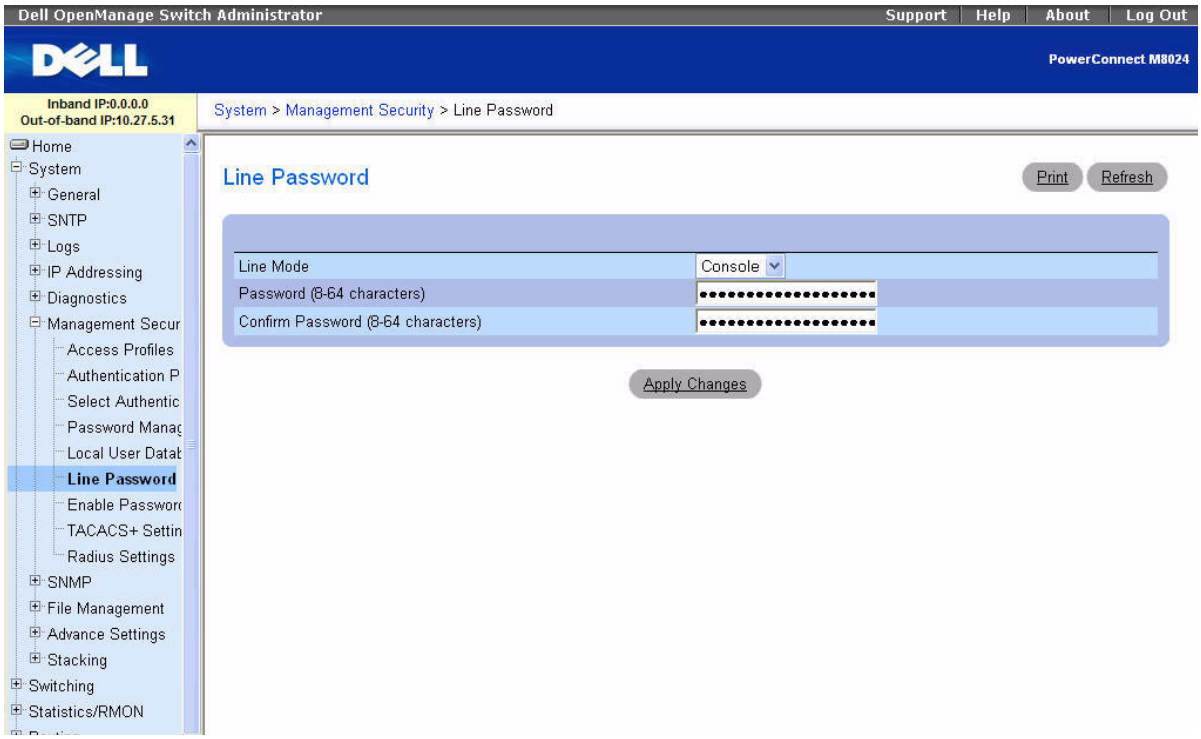
Line Passwords

Use the **Line Password** page to define line passwords for management methods.

To display the **Line Password** page, click **System > Management Security > Line Password** in the tree view.

Downloaded from www.Manualslib.com manuals search engine

Figure 6-51. Line Password



The **Line Password** page contains the following fields:

- **Line Mode —** Drop-down menu specifies device access through a Console, Telnet, or Secure Telnet (SSH) session.
- **Line Password (8 – 64 characters) —** The line password for accessing the device through a console, Telnet, or Secure Telnet session. The password appears in the ***** format.
- **Confirm Password (8 – 64 characters)** — Confirms the new line password. The password appears in the ***** format.

Defining Line Passwords

1. Open the **Line Password** page.
2. Select device access through a Console, Telnet, or Secure Telnet (SSH) session.
3. Define the **Line Password** field for the type of session you use to connect to the device.
4. Confirm the **Line Password**.
5. Click **Apply Changes**.

   The line password for the type of session is defined, and the device is updated.

Downloaded from www.Manualslib.com manuals search engine

Assigning Line Passwords Using CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

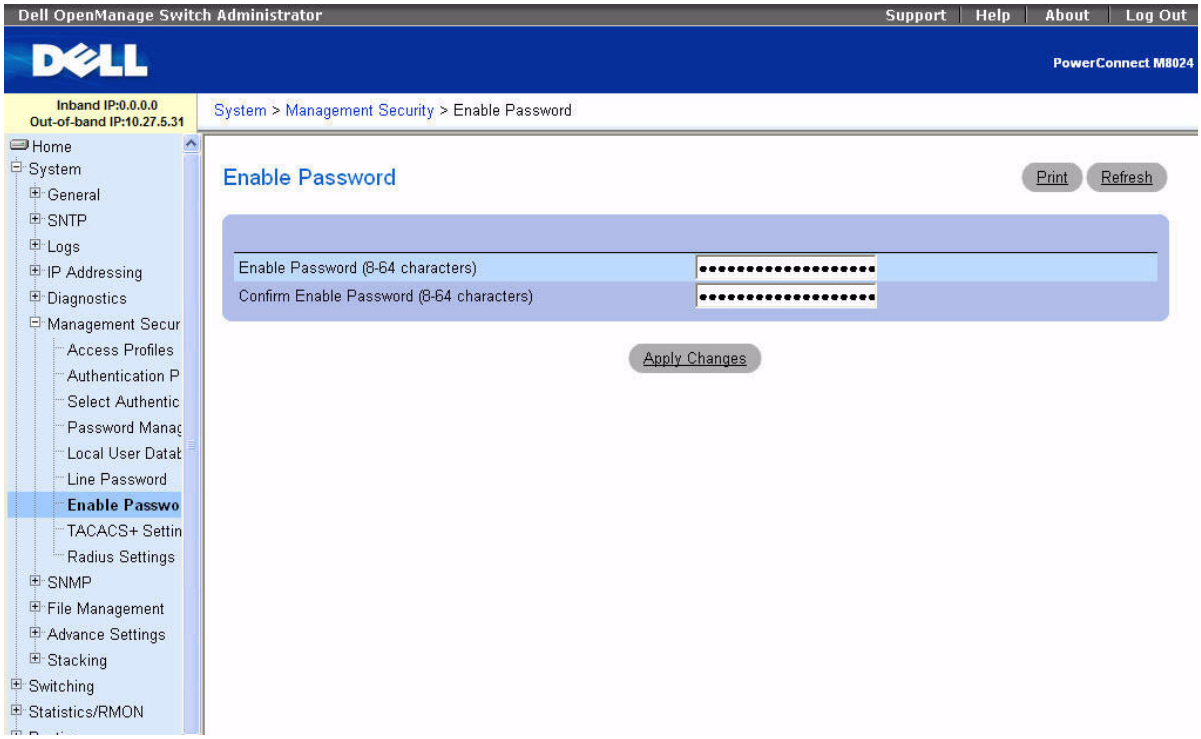
- AAA Commands.

Enable Password

Use the **Enable Password** page to set a local password to control access to normal and privilege levels.

To display the **Enable Password** page, click **System** > **Management Security** > **Enable Password** in the tree view.

Figure 6-52. Enable Password



The **Enable Password** page contains the following fields:

- **Enable Password (8–64 characters)** — The Enable password for controlling access to normal and privilege levels. The password appears in the ***** format.
- **Confirm Enable Password** — Confirms the new Enable password. The password appears in the ***** format.

Downloaded from www.Manualslib.com manuals search engine

Defining Enable Passwords

1. Open the **Enable Password** page.
2. Specify the Enable password.
3. Confirm the Enable password.
4. Click **Apply Changes**.

   The Enable password is set.

Assigning Enable Passwords Using CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- AAA Commands.

TACACS+ Settings

The device provide Terminal Access Controller Access Control System (TACACS+) client support. TACACS+ provides centralized security for validation of users accessing the device.

TACACS+ provides a centralized user management system, while still retaining consistency with RADIUS and other authentication processes. TACACS+ provides the following services:

- **Authentication —** Provides authentication during login and through user names and user-defined passwords.
- **Authorization —** Performed at login. Once the authentication session is completed, an authorization session starts using the authenticated user name. The TACACS+ server checks the user privileges.

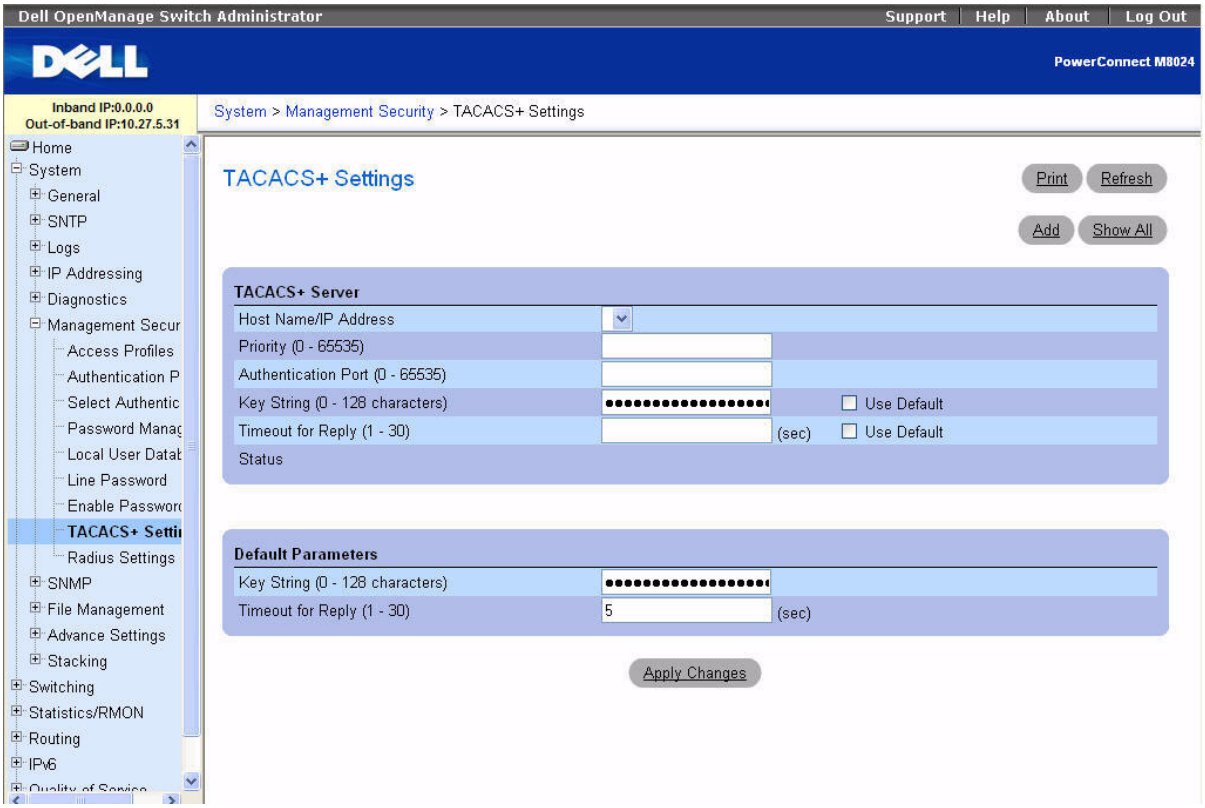
The TACACS+ protocol ensures network security through encrypted protocol exchanges between the device and TACACS+ server.

The **TACACS+ Settings** page contains both user-defined and the default TACACS+ settings for the inband management port.

To display the **TACACS+ Settings** page, click **System** > **Management Security** > **TACACS+** in the tree view.

Downloaded from www.Manualslib.com manuals search engine

Figure 6-53. TACACS+ Settings



The **TACACS+ Settings** page contains the following fields:

- **Host Name / IP Address** — Specifies the TACACS+ Server.
- **Priority** (0–65535) — Specifies the order in which the TACACS+ servers are used. The default is 0.
- **Authentication Port** (0–65535) — The port number through which the TACACS+ session occurs. The default is port 49.
- **Key String** (0–128 **Characters**) — Defines the authentication and encryption key for TACACS+ communications between the device and the TACACS+ server. This key must match the encryption used on the TACACS+ server. Check **Use Default** to use the default value.
- **Timeout for Reply** (1–30) — The amount of time that passes before the connection between the device and the TACACS+ server times out. The field range is from 1 to 30 seconds. Check **Use Default** to select the factory-default value.
- **Status** — The connection status between the device and the TACACS+ server. The possible field values are:
  - **Connected** — There is currently a connection between the device and the TACACS+ server.

Downloaded from www.Manualslib.com manuals search engine

– **Not Connected —** There is not currently a connection between the device and the TACACS+ server.

The fields in the Default Parameters section of the page contain values that are automatically applied to new TACACS+ servers.

- **Key String (0–128 Characters) —** Enter the default authentication and encryption key for TACACS+ communication between the device and the TACACS+ server.
- **Timeout for Reply (1–30) —** Enter the global user configuration time that passes before the connection between the device and the TACACS+ times out.

Defining TACACS+ Parameters

1. Open the **TACACS+ Settings** page.
2. Define the fields as needed.
3. Click **Apply Changes**.

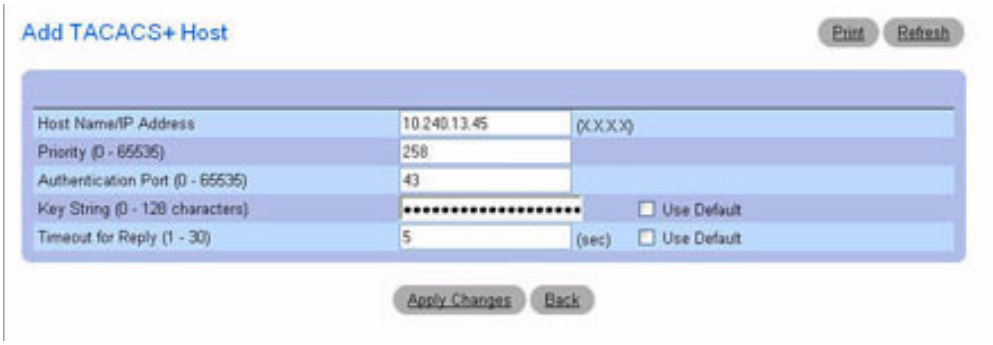
   The TACACS+ settings are updated to the device.

Adding a TACACS+ Server

1. Open the **TACACS+ Settings** page.
2. Click **Add**.

   The **Add TACACS+ Host** page displays.

Figure 6-54. Add TACACS+ Host



3. Define the fields as needed.
4. Click **Apply Changes**.

   The TACACS+ server is added, and the device is updated.

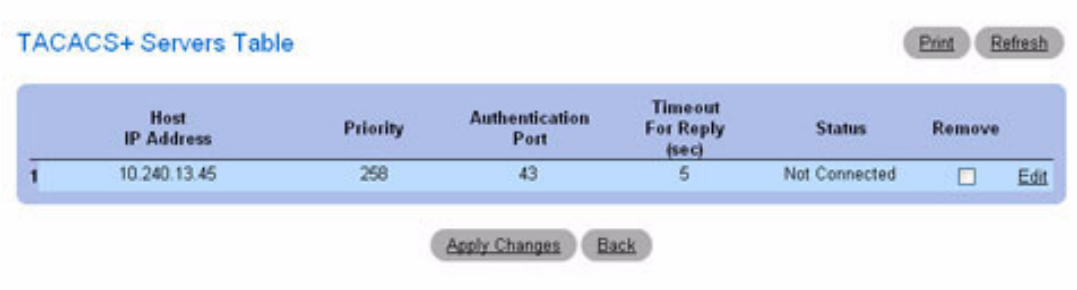
Displaying a TACACS+ Servers List

1. Open the **TACACS+ Settings** page.
2. Click **Show All**.

Downloaded from www.Manualslib.com manuals search engine

The **TACACS+ Servers Table** opens.

Figure 6-55. TACACS+ Servers Table



Removing a TACACS+ Server from the TACACS+ Servers List

1. Open the **TACACS+ Settings** page.
2. Click **Show All**.

   The **TACACS+ Servers Table** opens.
3. Select a **TACACS+ Servers Table** entry.
4. Select the **Remove** check box.
5. Click **Apply Changes**.

   The TACACS+ server is removed, and the device is updated.

Defining TACACS+ Servers Using CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- TACACS+ Commands.

RADIUS Global Configuration

The Remote Authorization Dial-In User Service (RADIUS) client on the PowerConnect M6220/M6348/M8024 switch supports multiple, named RADIUS servers. The RADIUS authentication and accounting server groups can contain one or more configured authentication servers that share the same RADIUS server name.

If you configure multiple RADIUS servers with the same RADIUS Server Name, designate one server as the primary and the other(s) as the backup server(s). The switch attempts to use the primary server first, and if the primary server does not respond, the switch attempts to use one of the backup servers with the same RADIUS Server Name.

The software also supports RADIUS Attribute 4, which is the configuration of a NAS-IP Address. The network access server (NAS) IP address is only used in Access-Request packets.

Downloaded from www.Manualslib.com manuals search engine

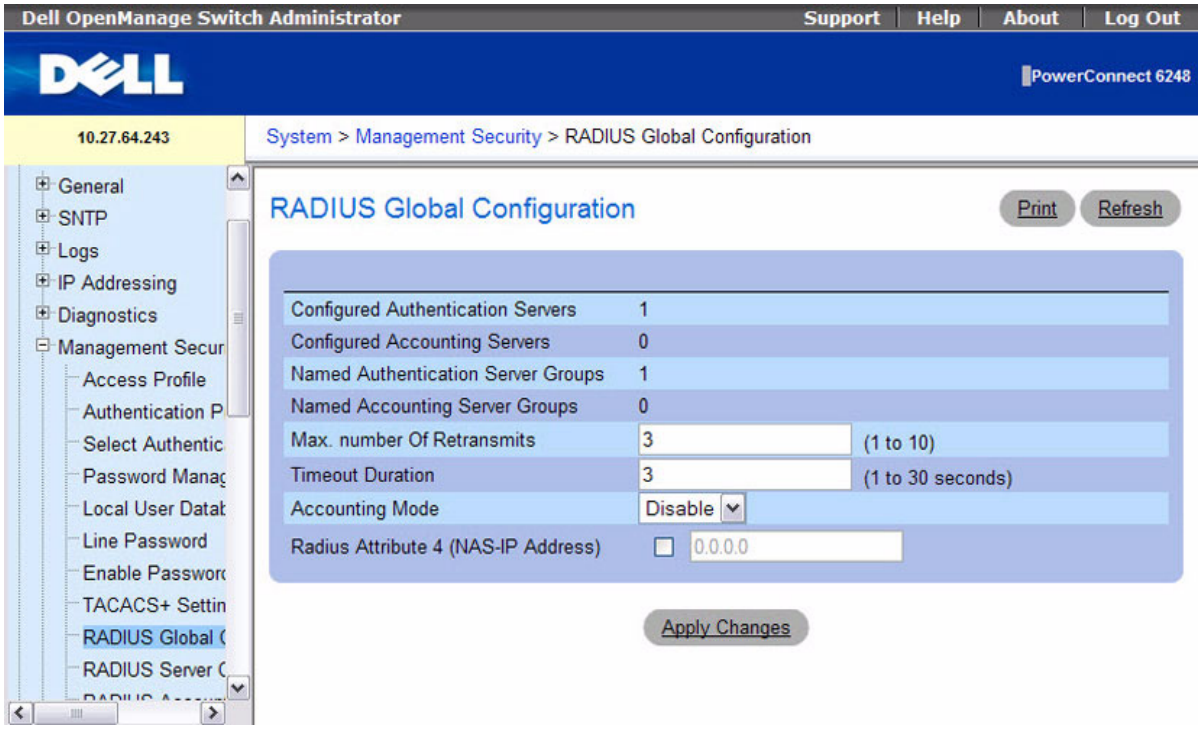
In some networks, the RADIUS server is responsible for assigning traffic to a particular VLAN. The RADIUS enhancements include the Authorization Network RADIUS feature that allows the switch to accept VLAN assignment by the RADIUS server.

The RADIUS server maintains a user database, which contains per-user authentication information. RADIUS servers provide a centralized authentication method for:

- Telnet Access
- Web Access
- Console to Switch Access
- Access Control Port (802.1x)

To display the **RADIUS Global Configuration** page, click **System > Management Security > RADIUS Global Configuration** in the tree view.

Figure 6-56. RADIUS Global Configuration



The **RADIUS Global Configuration** page contains the following fields:

- **Configured Authentication Servers** — The number of RADIUS authentication servers configured on the system. The value can range from 0 to 32.
- **Configured Accounting Servers** — The number of RADIUS accounting servers configured on the system. The value can range from 0 to 32.

Downloaded from www.Manualslib.com manuals search engine

- **Named Authentication Server Groups** — The number of authentication server groups configured on the system. An authentication server group contains one or more configured authentication servers that share the same RADIUS server name.
- **Named Accounting Server Groups** — The number of accounting server groups configured on the system. An accounting server group contains one or more configured authentication servers that share the same RADIUS server name.
- **Max Number of Retransmits** — The value of the maximum number of times a request packet is retransmitted. The valid range is 1-10. Consideration to maximum delay time should be given when configuring RADIUS max retransmit and RADIUS timeout. If multiple RADIUS servers are configured, the max retransmit value on each will be exhausted before the next server is attempted. A retransmit will not occur until the configured timeout value on that server has passed without a response from the RADIUS server. Therefore, the maximum delay in receiving a response from the RADIUS application equals the sum of (retransmit times timeout) for all configured servers. If the RADIUS request was generated by a user login attempt, all user interfaces will be blocked until the RADIUS application returns a response.
- **Timeout Duration** — The timeout value, in seconds, for request retransmissions. The valid range is 1 - 30. See the Max Number of Retransmits field description for more information about configuring the timeout duration.
- **Accounting Mode** — Use the menu to select whether the RADIUS accounting mode is enabled or disabled on the current server.
- **RADIUS Attribute 4 (NAS-IP Address)** — To set the network access server (NAS) IP address for the RADIUS server, select the option and enter the IP address of the NAS in the available field. The address should be unique to the NAS within the scope of the RADIUS server. The NAS IP address is only used in Access-Request packets.

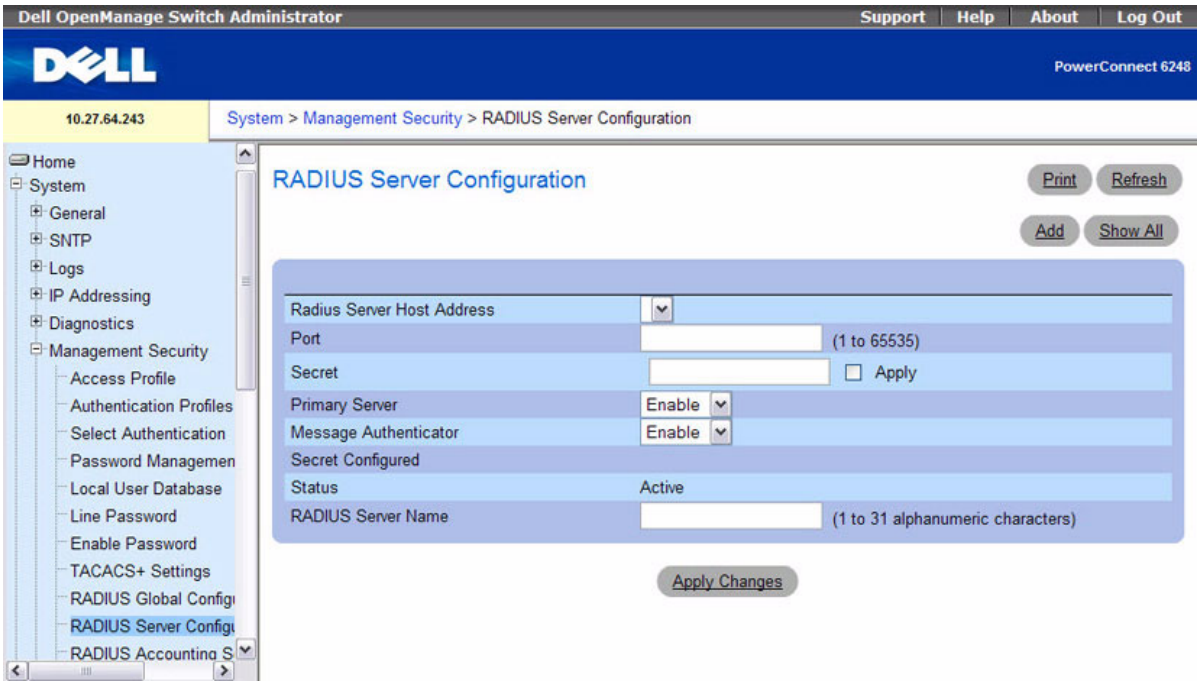
RADIUS Server Configuration

From the **RADIUS Server Configuration** page, you can add a new RADIUS server, configure settings for a new or existing RADIUS server, and view RADIUS server status information. The RADIUS client on the switch supports up to 32 named authentication and accounting servers.

To access the RADIUS Server Configuration page, click **System > Management Security > RADIUS Server Configuration** in the tree view.

Downloaded from www.Manualslib.com manuals search engine

Figure 6-57. RADIUS Server Configuration



The **RADIUS Server Configuration** page contains the following fields:

- **RADIUS Server Host Address** — Use the drop-down menu to select the IP address of the RADIUS server to view or configure. Click **Add** to display the Add RADIUS Server page used to configure additional RADIUS servers.
- **Port** — Identifies the authentication port the server uses to verify the RADIUS server authentication. The port is a UDP port, and the valid range is 1-65535. The default port for RADIUS authentication is 1812.
- **Secret** — Shared secret text string used for authenticating and encrypting all RADIUS communications between the device and the RADIUS server. This secret must match the RADIUS encryption.
- **Apply** — The Secret will only be applied if this box is checked. If the box is not checked, anything entered in the Secret field will have no affect and will not be retained. This field is only displayed if the user has READWRITE access.
- **Primary Server** — Sets the selected server to the Primary (**Enable**) or Secondary (**Disable**) server. If you configure multiple RADIUS servers with the same RADIUS Server Name, designate one server as the primary and the other(s) as the backup server(s). The switch attempts to use the primary server first, and if the primary server does not respond, the switch attempts to use one of the backup servers with the same RADIUS Server Name.

Downloaded from www.Manualslib.com manuals search engine

- **Message Authenticator** — Enable or disable the message authenticator attribute for the selected server.
- **Secret Configured** — Indicates whether the shared secret for this server has been configured.
- **Status** — Indicates whether the selected RADIUS server is currently serving as the active RADIUS server If more than one RADIUS server is configured with the same name, the switch selects one of the servers to be the active server from the group of servers with the same name. The status and can be one of the following:
  - **Active** — When the switch sends a RADIUS request to the named server, the request is directed to the server selected as the active server. Initially the primary server is selected as the active server. If the primary server fails, one of the other servers becomes the active server. If the primary server is not configured, the active server is the most recently configured RADIUS server.
  - **Inactive** — The server is a backup RADIUS server.
  - **RADIUS Server Name** — Shows the RADIUS server name.

To change the name, enter up to 32 alphanumeric characters. Spaces, hyphens, and underscores are also permitted. If you do not assign a name, the server is assigned the default name Default-RADIUS-Server.

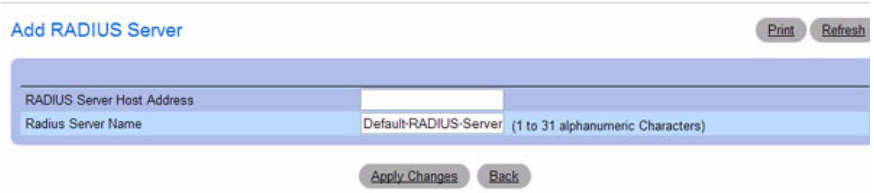
You can use the same name for multiple RADIUS Authentication servers. RADIUS clients can use RADIUS servers with the same name as backups for each other.

Adding a RADIUS Server

1. Open the **RADIUS Server Configuration** page.
2. Click **Add**.

   The **Add RADIUS Server** page displays.

Figure 6-58. Add RADIUS Server



3. Enter an IP address and name for the RADIUS server to add.
4. Click **Apply Changes**.

   The new RADIUS server is added, and the device is updated.

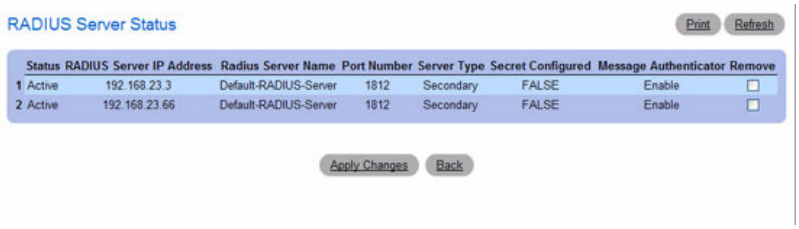
Downloaded from www.Manualslib.com manuals search engine

Viewing RADIUS Server Status and Removing a Named Server

1. Open the **RADIUS Server Configuration** page.
2. Click **Show All**.

   The **RADIUS Named Server Status** page displays.

Figure 6-59. RADIUS Server Status



	Status	RADIUS Server IP Address	Radius Server Name	Port Number	Server Type	Secret Configured	Message Authenticator	Remove
1	Active	192.168.23.3	Default-RADIUS-Server	1812	Secondary	FALSE	Enable	☐
2	Active	192.168.23.66	Default-RADIUS-Server	1812	Secondary	FALSE	Enable	☐

3. To remove a named server, select the check box in the **Remove** column.
4. Click **Apply Changes**.

   The RADIUS server is removed from the list.

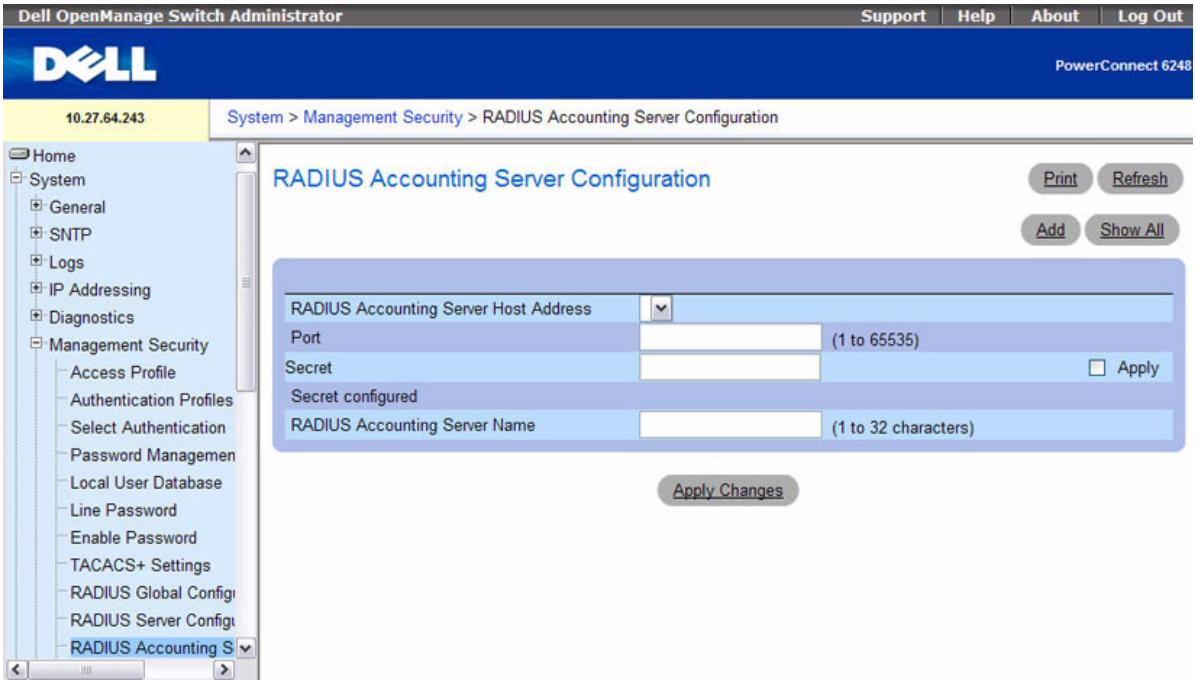
RADIUS Accounting Server Configuration

From the **RADIUS Accounting Server Configuration** page, you can add a new RADIUS accounting server, configure settings for a new or existing RADIUS accounting server, and view RADIUS accounting server status information. The RADIUS client on the switch supports up to 32 named authentication and accounting servers.

To access the RADIUS Server Configuration page, click **System > Management Security > RADIUS Accounting Server Configuration** in the tree view.

Downloaded from www.Manualslib.com manuals search engine

Figure 6-60. RADIUS Accounting Server Configuration



The **RADIUS Accounting Server Configuration** page contains the following fields:

- **RADIUS Accounting Server Host Address** — Use the drop-down menu to select the IP address of the accounting server to view or configure. Click **Add** to display the **Add RADIUS Accounting Server** page used to configure additional RADIUS servers.
- **Port** — Identifies the authentication port the server uses to verify the RADIUS accounting server authentication. The port is a UDP port, and the valid range is 1-65535. The default port for RADIUS accounting is 1813.
- **Secret** — Specifies the shared secret to use with the specified accounting server. This field is only displayed if you are logged into the switch with READWRITE access.
- **Apply** — The Secret will only be applied if this box is checked. If the box is not checked, anything entered in the Secret field will have no affect and will not be retained. This field is only displayed if you are logged into the switch with READWRITE access.
- **Secret Configured** — Indicates whether the shared secret for this server has been configured.
- **RADIUS Accounting Server Name** — Enter the name of the RADIUS accounting server. The name can contain from 1 to to 32 alphanumeric characters. Hyphens, and underscores are also permitted.

  You can use the same name for multiple RADIUS accounting servers. RADIUS clients can use accounting servers with the same name as backups for each other.

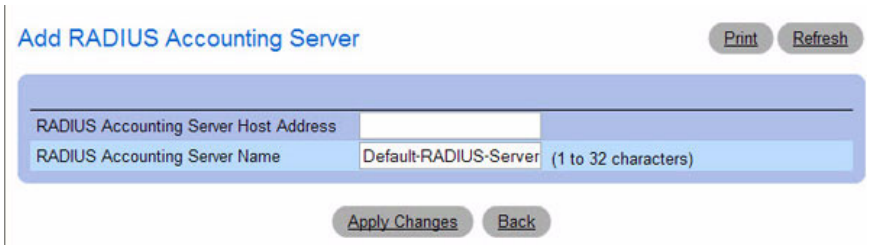
Downloaded from www.Manualslib.com manuals search engine

Adding a RADIUS Accounting Server

1. Open the **RADIUS Accounting Server Configuration** page.
2. Click **Add**.

   The **Add RADIUS Accounting Server** page displays.

Figure 6-61. Add RADIUS Accounting Server



3. Enter an IP address and name for the RADIUS accounting server to add.
4. Click **Apply Changes**.

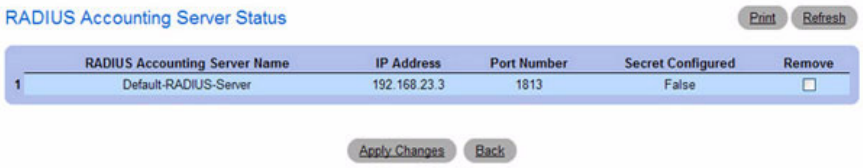
   The new RADIUS server is added, and the device is updated.

Viewing RADIUS Accounting Server Status and Removing a Accounting Named Server

1. Open the **RADIUS Accounting Server Configuration** page.
2. Click **Show All**.

   The **RADIUS Named Accounting Server Status** page displays.

Figure 6-62. RADIUS Accounting Server Status



3. To remove a named accounting server, select the check box in the **Remove** column.
4. Click **Apply Changes**.

   The RADIUS accounting server is removed from the list.

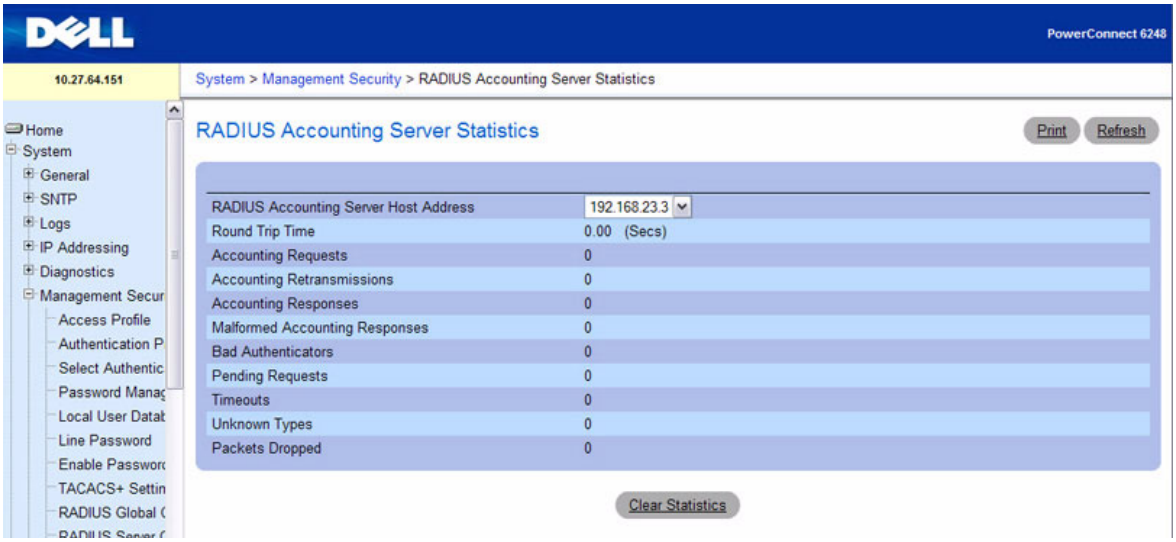
Downloaded from www.Manualslib.com manuals search engine

RADIUS Accounting Server Statistics

Use the **RADIUS Accounting Server Statistics** page to view statistical information for each RADIUS accounting server configured on the system.

To access the RADIUS Accounting Server Statistics page, click **System** > **Management Security** > **RADIUS Accounting Server Statistics** in the tree view.

Figure 6-63. RADIUS Accounting Server Statistics



The **RADIUS Accounting Server Statistics** page contains the following fields:

- **RADIUS Accounting Server Host Address** — Use the drop-down menu to select the IP address of the RADIUS accounting server for which to display statistics.
- **Round Trip Time** — Displays the time interval, in hundredths of a second, between the most recent Accounting-Response and the Accounting-Request that matched it from this RADIUS accounting server.
- **Accounting Requests** — The number of RADIUS Accounting-Request packets sent to this server. This number does not include retransmissions.
- **Accounting Retransmissions** — The number of RADIUS Accounting-Request packets retransmitted to this server.
- **Accounting Responses** — Displays the number of RADIUS packets received on the accounting port from this server.
- **Malformed Accounting Responses** — Displays the number of malformed RADIUS Accounting-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators and unknown types are not included as malformed accounting responses.
- **Bad Authenticators** — Displays the number of RADIUS Accounting-Response packets that contained invalid authenticators received from this accounting server.

Downloaded from www.Manualslib.com manuals search engine

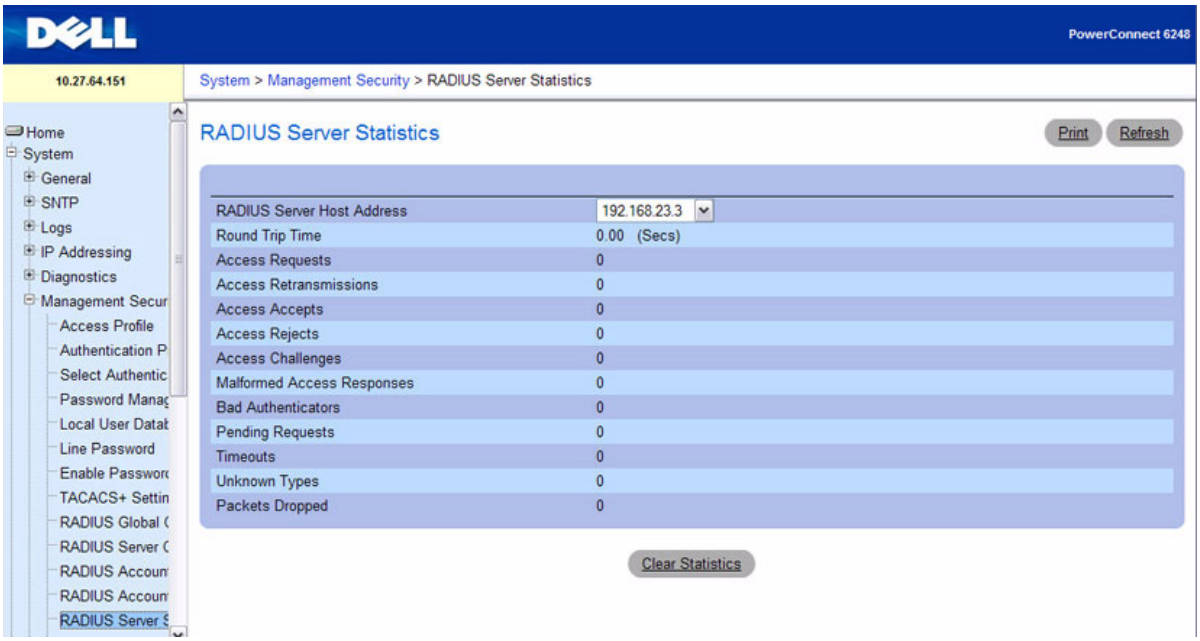
- **Pending Requests** — The number of RADIUS Accounting-Request packets destined for this server that have not yet timed out or received a response.
- **Timeouts** — The number of accounting timeouts to this server.
- **Unknown Types** — The number of RADIUS packets of unknown type which were received from this server on the accounting port.
- **Packets Dropped** — The number of RADIUS packets received from this server on the accounting port and dropped for some other reason.

RADIUS Server Statistics

Use the **RADIUS Server Statistics** page to view statistical information for each RADIUS server configured on the system.

To access the RADIUS Server Statistics page, click **System > Management Security > RADIUS Server Statistics** in the tree view.

Figure 6-64. RADIUS Server Statistics



The **RADIUS Server Statistics** page contains the following fields:

- **RADIUS Server Host Address** — Use the drop-down menu to select the IP address of the RADIUS server for which to display statistics.
- **Round Trip Time** — The time interval, in hundredths of a second, between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from this RADIUS authentication server.

Downloaded from www.Manualslib.com manuals search engine

- **Access Requests** — The number of RADIUS Access-Request packets sent to this server. This number does not include retransmissions.
- **Access Retransmissions** — The number of RADIUS Access-Request packets retransmitted to this server.
- **Access Accepts** — The number of RADIUS Access-Accept packets, including both valid and invalid packets, that were received from this server.
- **Access Rejects** — The number of RADIUS Access-Reject packets, including both valid and invalid packets, that were received from this server.
- **Access Challenges** — The number of RADIUS Access-Challenge packets, including both valid and invalid packets, that were received from this server.
- **Malformed Access Responses** — The number of malformed RADIUS Access-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators or signature attributes or unknown types are not included as malformed access-responses.
- **Bad Authenticators** — The number of RADIUS Access-Response packets containing invalid authenticators or signature attributes received from this server.
- **Pending Requests** — The number of RADIUS Access-Request packets destined for this server that have not yet timed out or received a response.
- **Timeouts** — The number of authentication timeouts to this server.
- **Unknown Types** — The number of RADIUS packets of unknown type which were received from this server on the authentication port.
- **Packets Dropped** — The number of RADIUS packets received from this server on the authentication port and dropped for some other reason.

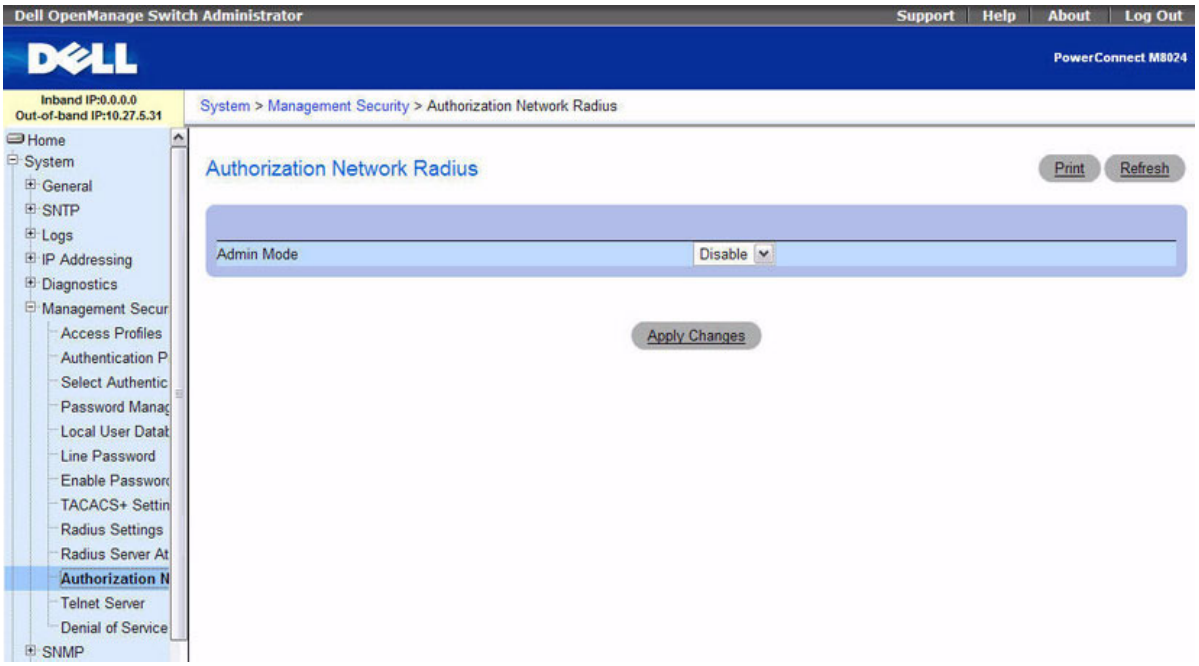
Authorization Network RADIUS

In some networks, the RADIUS server is responsible for assigning traffic to a particular VLAN. From the **Authorization Network RADIUS** page, you can enable the switch to accept VLAN assignment by the RADIUS server.

To display the **Authorization Network RADIUS** page, click **System Management > Security > Authorization Network RADIUS** in the tree view.

Downloaded from www.Manualslib.com manuals search engine

Figure 6-65. Authorization Network RADIUS



The **Authorization Network RADIUS** page contains the following field:

- **Admin Mode**— Enables or disables the ability of the switch to accept VLAN assignment from the RADIUS server.

Downloaded from www.Manualslib.com manuals search engine

Telnet Server

Use the **Telnet Server** page to enable or disable telnet service on the switch or to modify the telnet port. To display the **Telnet Server** page, click **System** > **Management Security** > **Telnet Server**.

Figure 6-66. Telnet Server

The **Telnet Server** page contains the following fields:

- **New Telnet Sessions** — Controls the administrative mode for inbound telnet sessions. If you set the mode to Block, new telnet sessions are not allowed, but existing sessions are not interrupted. The default value is Allow.
- **Telnet Port Number** — Port number on which telnet session can be initiated. This port will be used for new inbound Telnet session on the switch. After you modify the telnet server port, new inbound telnet sessions use the new port and existing telnet sessions are not affected.

Modifying Telnet Server Settings

1. Open the **Telnet Server Configuration** page.
2. Configure the relevant fields.
3. Click **Apply Changes**.

   The settings are saved, and the device is updated.

Downloaded from www.Manualslib.com manuals search engine

Configuring the Telnet Server Using CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

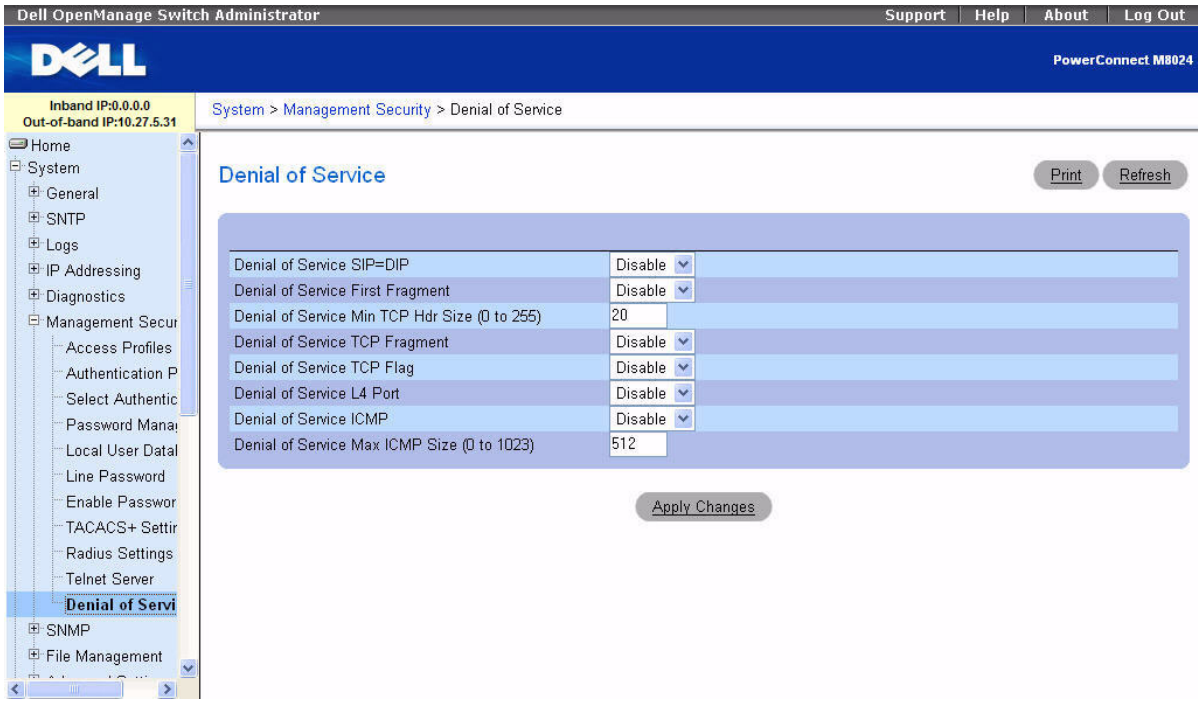
- Telnet Server Commands

Denial of Service

Denial of Service refers to the exploitation of a variety of vulnerabilities which would interrupt the service of a host or make a network unstable. Use the **Denial of Service** page to configure settings to help prevent denial of service attacks.

To display the **Denial of Service** page, click **System** > **Management Security** > **Denial of Service** in the tree view.

Figure 6-67. Denial of Service



The **Denial of Service** page contains the following fields:

- **Denial of Service SIP=DIP** — Enabling SIP=DIP DoS prevention causes the switch to drop packets that have a source IP address equal to the destination IP address.
- **Denial of Service First Fragment** — Enabling First Fragment DoS prevention causes the switch to drop packets that have a TCP header smaller than the configured minimum TCP header size (Min TCP Hdr Size).

Downloaded from www.Manualslib.com manuals search engine

- **Denial of Service Min TCP Hdr Size** — Specify the minimum TCP header size allowed. If First Fragment DoS prevention is enabled, the switch will drop packets that have a TCP header smaller then this configured value.
- **Denial of Service TCP Fragment** — Enabling TCP Fragment DoS prevention causes the switch to drop packets that have an IP fragment offset equal to one.
- **Denial of Service TCP Flag** — Enabling TCP Flag DoS prevention causes the switch to drop packets that meet any of the following conditions:
  - TCP flag SYN set and TCP source port less than 1024
  - TCP control flags set to 0 and TCP sequence number set to 0
  - TCP flags FIN, URG, and PSH set and TCP sequence number set to 0
  - Both TCP flags SYN and FIN set
- **Denial of Service L4 Port** — Enabling L4 Port DoS prevention causes the switch to drop packets that have the TCP/UDP source port equal to TCP/UDP destination port.
- **Denial of Service ICMP** — Enabling ICMP DoS prevention causes the switch to drop ICMP packets that have a type set to ECHO_REQ (ping) and a size greater than the configured ICMP packet size (ICMP Pkt Size).
- **Denial of Service Max ICMP Pkt Size** — Specify the maximum ICMP packet size to allow. If ICMP DoS prevention is enabled, the switch will drop ICMP ping packets that have a size greater then this configured value.

Configuring Denial of Service Settings

1. Open the **Denial of Service** page.
2. Specify the desired settings.
3. Click **Apply Changes**.

   The device is updated with the new settings.

Configuring Denial of Service Settings Using CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- Denial of Service Commands.

Downloaded from www.Manualslib.com manuals search engine

Captive Portal

The Captive Portal (CP) feature allows you to block clients directly connected to the switch from accessing the network until user verification has been established. You can configure CP verification to allow access for both guest and authenticated users. Authenticated users must be validated against a database of authorized Captive Portal users before access is granted. The database can be stored locally on the switch or on a RADIUS server.

When a port is enabled for Captive Portal, all the traffic coming onto the port from the unauthenticated clients are dropped except for the ARP, DHCP, DNS and NETBIOS packets. These packets are allowed to be forwarded by the switch so that the unauthenticated clients can get an IP address and be able to resolve the hostname or domain names. Data traffic from authenticated clients goes through as expected. If an unauthenticated client opens a web browser and tries to connect to network, the Captive Portal redirects all the HTTP/HTTPS traffic from unauthenticated clients to the authenticating server on the switch. A Captive portal web page is sent back to the unauthenticated client and the client can authenticate and based upon the authentication the client is given access to the port.

NOTE: For information about the CLI commands you use to view and configure Captive Portal settings, refer to the Captive Portal Commands chapter in the CLI Reference Guide:

The Captive Portal folder contains links to the following pages that help you view and configure system Captive Portal settings:

- CP Global Configuration
- CP Configuration
- CP Web Customization
- Local User
- User Group
- Interface Association
- CP Status
- CP Activation and Activity Status
- Interface Activation Status
- Interface Capability Status
- Client Summary
- Client Detail
- CP Interface Client Status
- CP Client Status

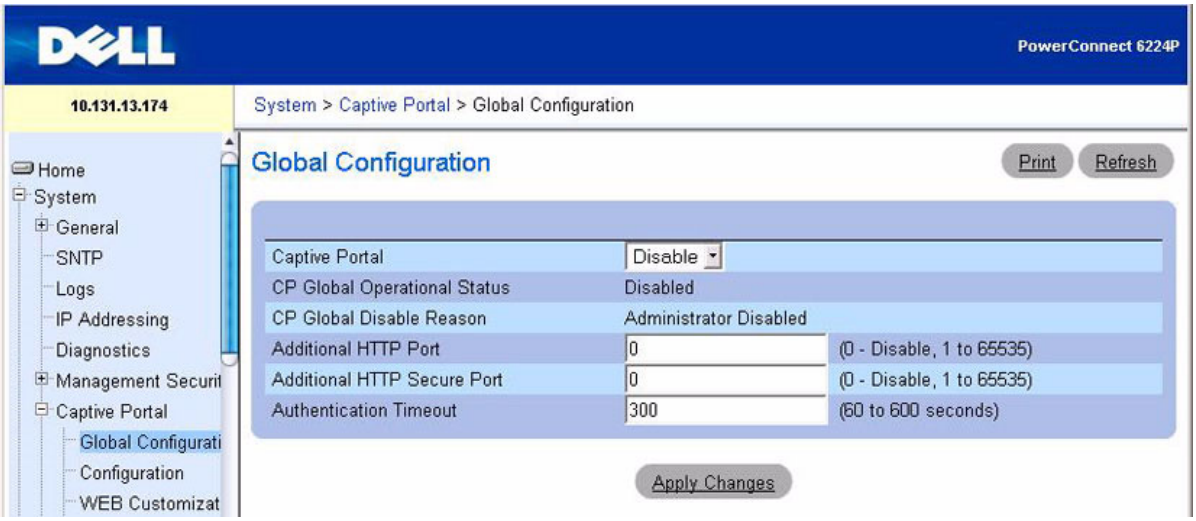
Downloaded from www.Manualslib.com manuals search engine

CP Global Configuration

From the **CP Global Configuration** page, you can control the administrative state of the CP feature and configure global settings that affect all captive portals configured on the switch.

To configure the global CP settings, click **System > Captive Portal > Global Configuration**.

Figure 6-68. CP Global Configuration



The **CP Global Configuration** page contains the following fields:

- **Captive Portal** — Enable or disable the CP feature on the switch.
- **CP Global Operational Status** — Shows whether the CP feature is enabled.
- **CP Global Disable Reason** — If CP is disabled, this field displays the reason, which can be one of the following:
  - None
  - Administrator Disabled
  - No IPv4 Address
  - Routing Enabled, but no IPv4 routing interface
- **Additional HTTP Port** — HTTP traffic uses port 80, but you can configure an additional port for HTTP traffic. Enter a port number between 0-65535 (excluding ports 80, 443, and the configured switch management port).
- **Additional HTTP Secure Port** — HTTP traffic over SSL (HTTPS) uses port 443, but you can configure an additional port for HTTPS traffic. Enter a port number between 0-65535 (excluding ports 80, 443, and the configured switch management port).

Downloaded from www.Manualslib.com manuals search engine

- **Authentication Timeout** — To access the network through a portal, the client must first enter authentication information on an authentication Web page. Enter the number of seconds to keep the authentication session open with the client. When the timeout expires, the switch disconnects any active TCP or SSL connection with the client.

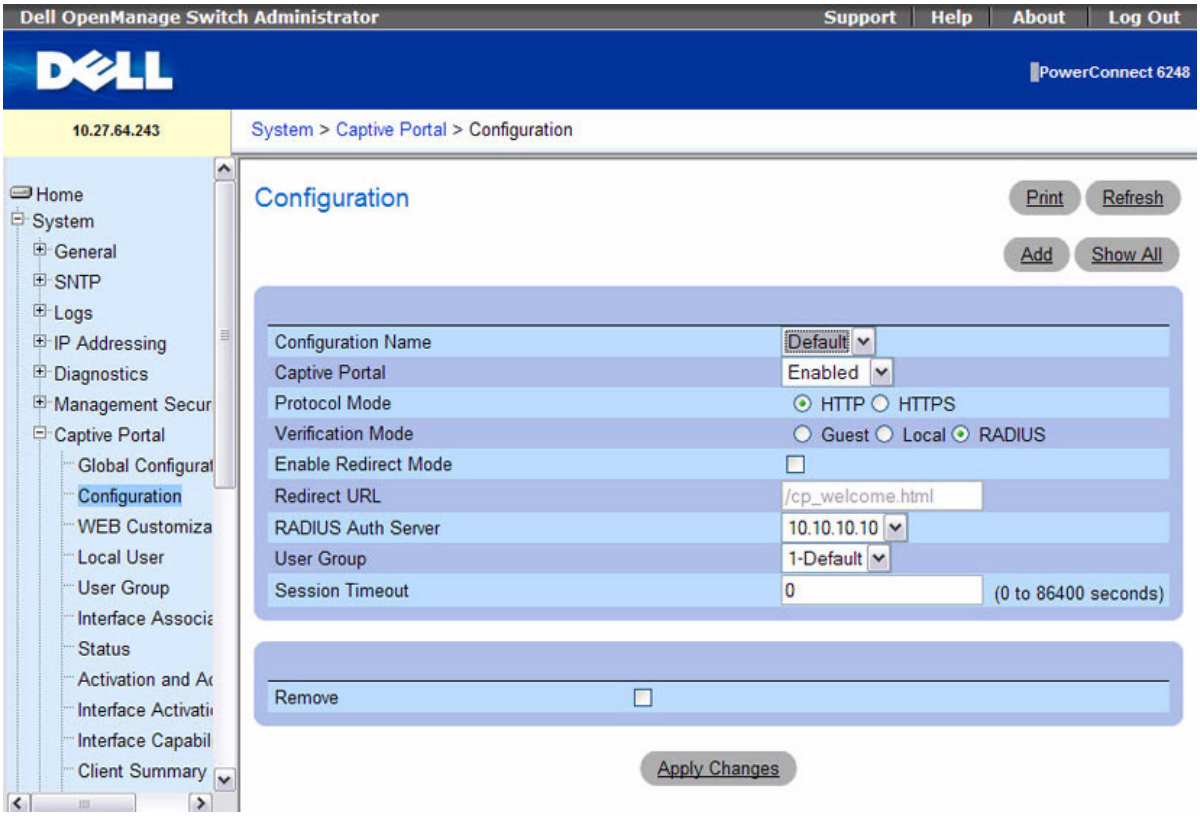
CP Configuration

From the **CP Configuration** page, you can view summary information about captive portals on the system, add a captive portal, and configure existing captive portals.

The switch supports 10 CP configurations. CP configuration 1 is created by default and can not be deleted. Each captive portal configuration can have unique guest or group access modes and a customized acceptance use policy that displays when the client connects.

To view summary information about existing captive portals, or to add or delete a captive portal, click **System > Captive Portal > Configuration**.

Figure 6-69. CP Configuration



Downloaded from www.Manualslib.com manuals search engine

The **CP Configuration** page contains the following fields:

- **Configuration Name** — If multiple CP configurations exist on the system, select the CP configuration to view or configure. Use the **Add** button to add a new CP configuration to the switch.
- **Captive Portal** — Use this field to enable or disable the selected CP configuration.
- **Protocol Mode** — Choose whether to use HTTP or HTTPS as the protocol for the portal to use during the verification process.
  - **HTTP** — Does not use encryption during verification
  - **HTTPS** — Uses the Secure Sockets Layer (SSL), which requires a certificate to provide encryption. The certificate is presented to the user at connection time.
- **Verification Mode** — Select the mode for the CP to use to verify clients:
  - **Guest** — The user does not need to be authenticated by a database.
  - **Local** — The switch uses a local database to authenticated users.
  - **RADIUS** — The switch uses a database on a remote RADIUS server to authenticate users.

  NOTE: To configure authorized users on the local or remote RADIUS database, see "Local User" on page 194.
- **Enable Redirect Mode** — Select this option to specify that the CP should redirect the newly authenticated client to the configured URL. If this option is clear, the user sees the welcome page after a successful verification.
- **Redirect URL** — Specify the URL to which the newly authenticated client is redirected if the URL Redirect Mode is enabled.
- **RADIUS Auth Server** — If the verification mode is RADIUS, click the drop-down menu and select the name of the RADIUS server used for client authentications. The switch acts as the RADIUS client and performs all RADIUS transactions on behalf of the clients. To configure RADIUS server information, go to the **Management Security > RADIUS Server Configuration** page.
- **User Group** — If the Verification Mode is Local or RADIUS, assign an existing User Group to the captive portal or create a new group. All users who belong to the group are permitted to access the network through this portal. The User Group list is the same for all CP configurations on the switch.
- **Session Timeout** — Enter the number of seconds to wait before terminating a session. A user is logged out once the session timeout is reached. If the value is set to 0 then the timeout is not enforced. The default value is 0. The range is 0 to 86400 seconds.

Removing a Captive Portal Configuration

1. To remove a CP configuration, select the CP configuration to remove from the Configuration Name menu.
2. Select the **Remove** option at the bottom of the page.
3. Click **Apply Changes**.

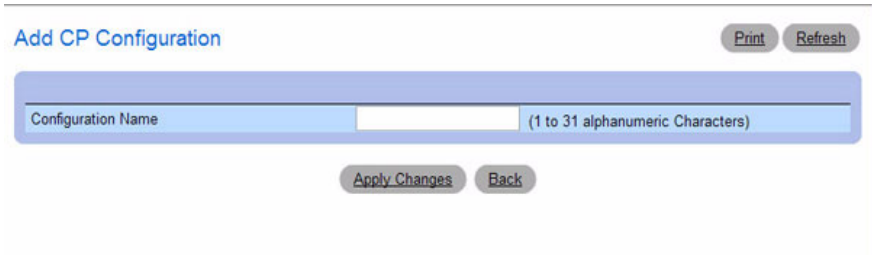
Downloaded from www.Manualslib.com manuals search engine

Adding a Captive Portal Configuration

1. Open the **Captive Portal Configuration** page.
2. Click **Add**.

   The **Add CP Configuration page** displays:

Figure 6-70. Add CP Configuration



3. Enter a name for the new CP configuration.
4. Click **Apply Changes**.

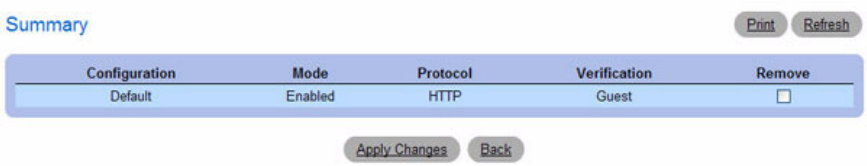
   The CP configuration is added, and the device is updated.

Displaying the CP Configuration Summary

1. Open the Captive Portal **Configuration** page.
2. Click **Show All**.

   The **CP Summary** page displays:

Figure 6-71. CP Summary



3. To remove a CP configuration, select the **Remove** option in the CP configuration row and click **Apply Changes**.

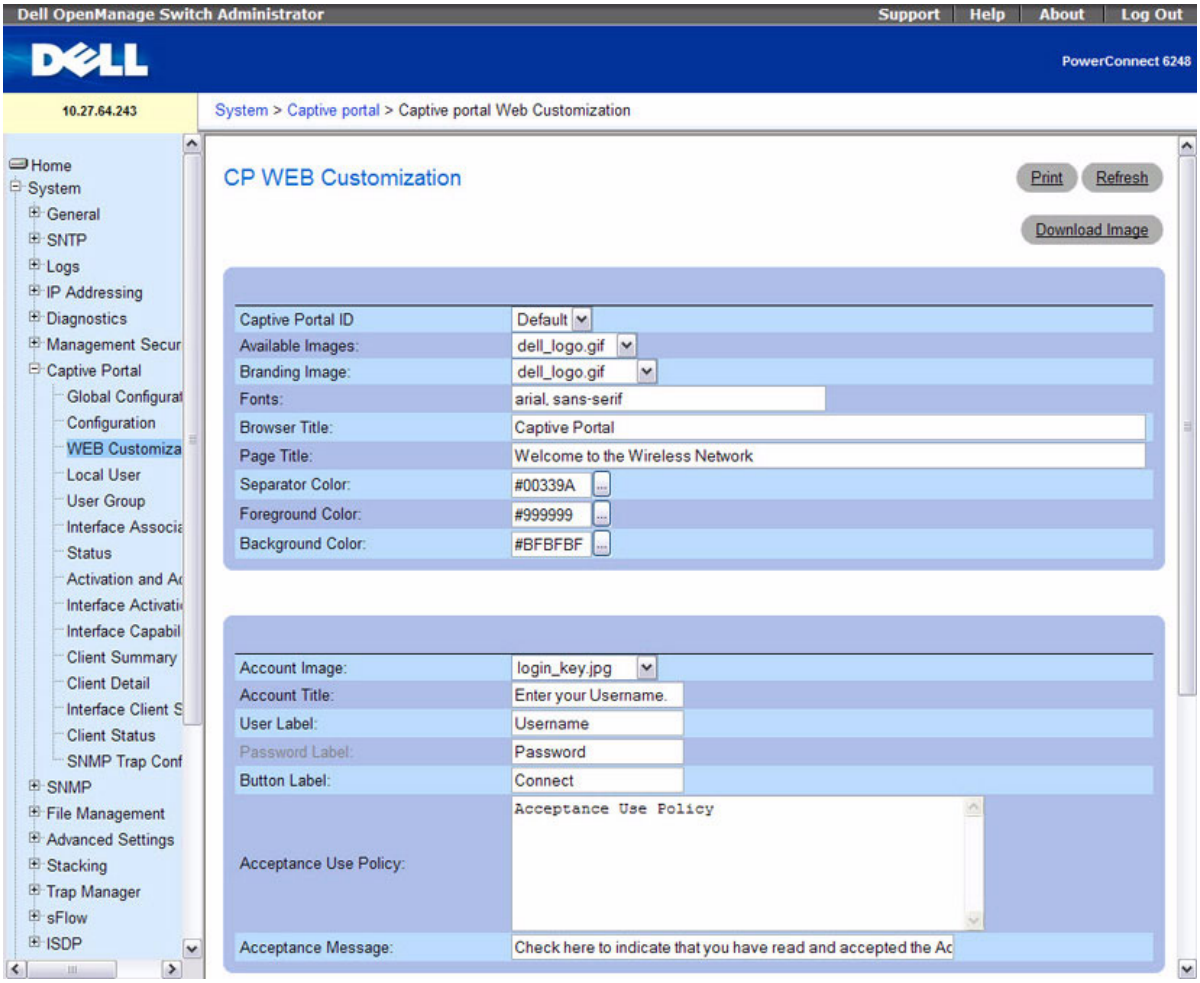
Downloaded from www.Manualslib.com manuals search engine

CP Web Customization

When a client connects to the access point, the user sees a Web page. The **CP Web Customization** page allows you to customize the appearance of that page with specific text and images. To display the **CP Web Customization** page, click **System > Captive Portal > Web Customization.**

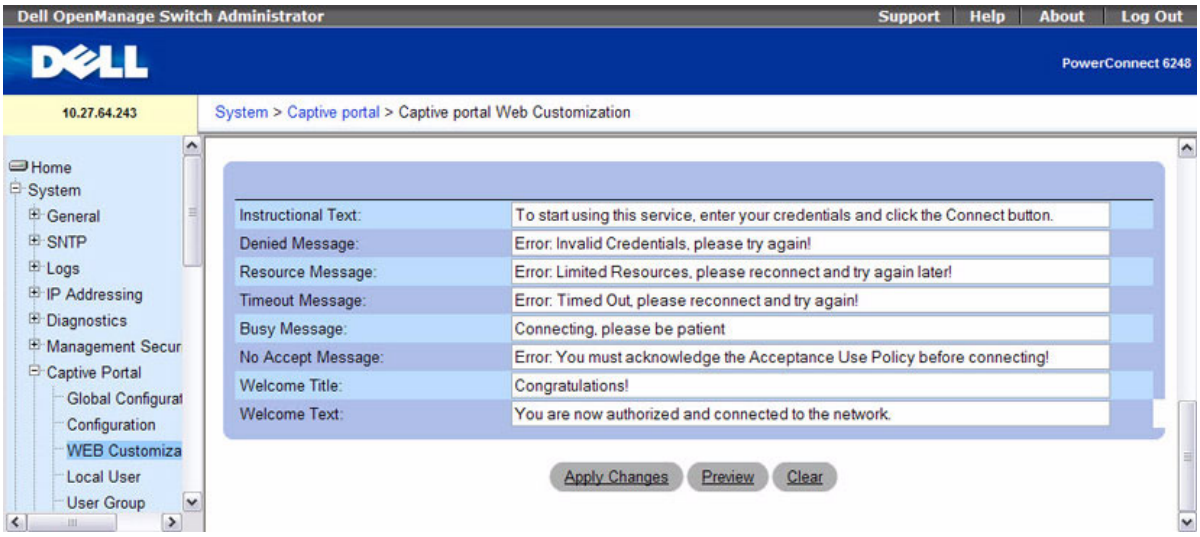
To configure the portal users in a remote RADIUS server, see "Configuring Users in a Remote RADIUS Server" on page 196.

Figure 6-72. CP Web Customization



Downloaded from www.Manualslib.com manuals search engine

Figure 6-73. CP Web Customization (cont.)



The **CP Web Customization** page contains the following fields:

- **Captive Portal ID** — The drop-down menu lists each CP configured on the switch. To view information about the clients connected to the CP, select it from the list.
- **Branding Image** — Select the name of the image file to display on the top left corner of the page. This image is used for branding purposes, such as the company logo.
- **Fonts** — Enter the name of the font to use for all text on the CP page.
- **Browser Title** — Enter the text to display on the client's Web browser title bar or tab.
- **Page Title** — Enter the text to use as the page title. This is the text that identifies the page.
- **Separator Color** — Enter the hexadecimal color code to use as the separator above and below the login area and acceptance use policy. Press the ... button for a color pick list. The sample account information is updated with the colors you choose.
- **Foreground Color**— Enter the hexadecimal color code to use as the foreground color in the login area. Press the ... button for a color pick list. The sample account information is updated with the colors you choose.
- **Background Color** — Enter the hexadecimal color code to as the background color in the login area. Press the ... button for a color pick list. The sample account information is updated with the colors you choose.
- **Account Image** — Select the image that will display on the Captive Portal page above the login field. The image display area is 55H X 310W pixels. Your image will be resized to fit the display area. Click **Download Image**, then browse to and select an image on your local system (or accessible from your local system) to download to the switch.
- **Account Title** — Enter the summary text to display that instructs users to authenticate.

Downloaded from www.Manualslib.com manuals search engine

- **User Label** — Enter the text to display next to the field where the user enters the username.
- **Password Label** — Enter the text to display next to the field where the user enters the password.
- **Button Label** — Enter the text to display on the button the user clicks to connect to the network.
- **Acceptance Use Policy** — Enter the text to display in the Acceptance Use Policy field. The acceptance use policy instructs users about the conditions under which they are allowed to access the network. The policy can contain up to 128 characters.
- **Acceptance Message** — Enter the text to display next to the box that the user must select to indicate that he or she accepts the terms of use.
- **Instructional Text** — Enter the detailed text to display that instructs users to authenticate. This text appears under the button.
- **Denied Message** — Enter the text to display when the user does not provide valid authentication information. This message displays after the user clicks the button to connect to the network.
- **Resource Message** — Enter the text to display when the system has rejected authentication due to system resource limitations. This message displays after the user clicks the button to connect to the network.
- **Timeout Message** — Enter the text to display when the system has rejected authentication because the authentication transaction took too long. This could be due to user input time, or a timeout due to the overall transaction.
- **Busy Message** — Enter the text to display when the user does not provide valid authentication information. This message displays after the user clicks the button to connect to the network.
- **No Accept Message** — Enter the text to display when the user did not accept the acceptance use policy. This message displays after the user clicks the button to connect to the network.
- **Welcome Title** — Enter the title to display to greet the user after he or she successfully connects to the network.
- **Welcome Text** — Enter the optional text to display to further identify the network to be access by the CP user. This message displays under the Welcome Title.

Previewing and Resetting the CP Web Page

To preview the custom CP Web page, click **Preview**.

To reset the CP Web page to the default settings, click **Clear**.

Downloaded from www.Manualslib.com manuals search engine

Local User

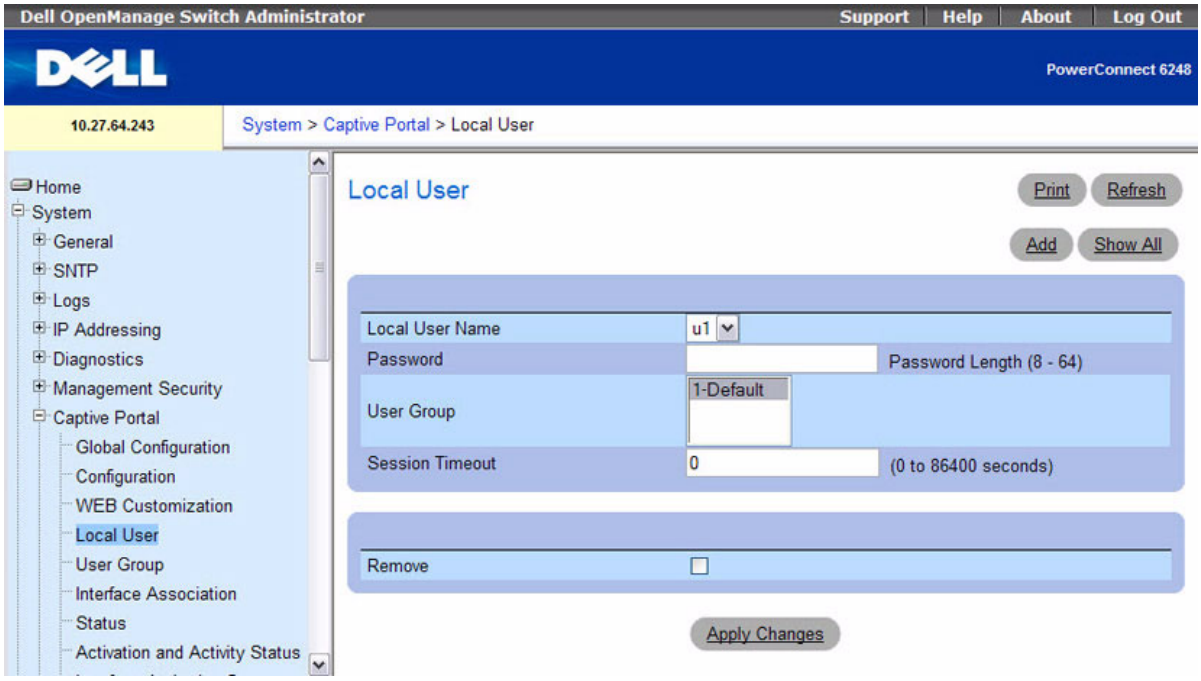
You can configure a portal to accommodate guest users and authorized users. Guest users do not have assigned user names and passwords. Authorized users provide a valid user name and password that must first be validated against a local database or RADIUS server. Authorized users can gain network access once the switch confirms the user's credentials.

The **Local User** page allows you to add authorized users to the local database, which can contain up to 1024 user entries. You can also add and delete users from the local database from the Local User page.

To view and configure CP users in the local database, click **System > Captive Portal > Local User**.

The following figure shows the **Local User** page after a user has been added. If no users have been added to the switch, many of the fields do not display on the screen.

Figure 6-74. Local User Configuration



The **Local User** page contains the following fields:

- **Local User Name** — Enter the name of the user.
- **Password** — Enter a password for the user. The password length can be from 8 to 64 characters.
- **User Group** — Assign the user to at least one User Group. New users are assigned to the 1-Default user group by default.
- **Session Timeout** — Enter the number of seconds a user is permitted to remain connected to the network. Once the Session Timeout value is reached, the user is logged out automatically. A value of 0 means that the user does not have a Session Timeout limit.

Downloaded from www.Manualslib.com manuals search engine

Removing a Local User

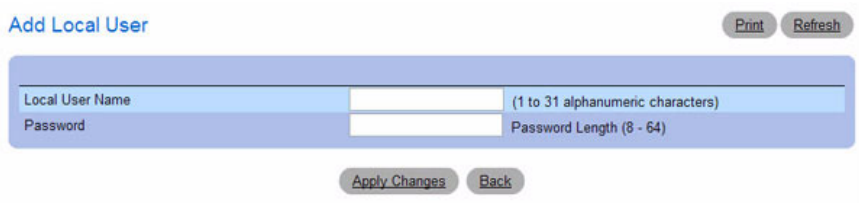
1. Select the user from the **Local User Name** field.
2. Select the **Remove** option at the bottom of the page.
3. Click **Apply Changes** to remove the user.

Adding a Local User

1. Open the **Local User** page.
2. Click **Add**.

   The **Add Local User** page displays:

Figure 6-75. Add Local User



3. Enter a name for the new user. The name is 1 to 31 alphanumeric characters.
4. Enter a password for the new user. The password is 8-64 characters in length.
5. Click **Apply Changes**.

   The local user is added, and the device is updated.

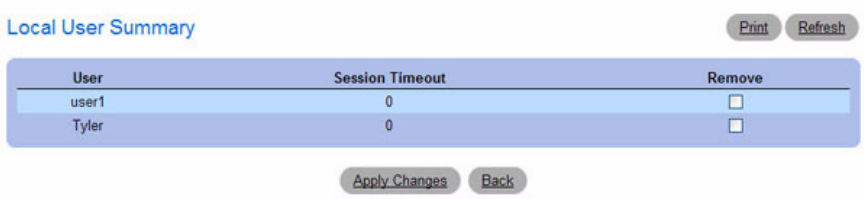
   If no user is added, a No User Exists message is shown in the web page instead of the empty controls.

Displaying the Local User Summary Page

1. Open the **Local User** page.
2. Click **Show All**.

   The **CP Local User Summary** page displays:

Figure 6-76. CP Local User Summary



3. To remove a configured user, select the **Remove** option in the appropriate row, and then click **Apply Changes**.

Downloaded from www.Manualslib.com manuals search engine

Configuring Users in a Remote RADIUS Server

You can use a remote RADIUS server client authorization. You must add all users to the RADIUS server. The local database does not share any information with the remote RADIUS database.

The following table indicates the RADIUS attributes you use to configure authorized captive portal clients. The table indicates both RADIUS attributes and vendor-specific attributes (VSA). VSAs are denoted in the Attribute column and are comma delimited (vendor id, attribute id).

Table 6-1. Captive Portal User RADIUS Attributes

Attribute	Number	Description	Range	Usage	Default
User-Name	1	User name to be authorized	1-32 characters	Required	None
User-Password	2	User password	8-64 characters	Required	None
Session-Timeout	27	Logout once session timeout is reached (seconds). If the attribute is 0 or not present then use the value configured for the captive portal.	Integer (seconds)	Optional	0
Idle-Timeout	28	Logout once idle timeout is reached (seconds). If the attribute is 0 or not present then use the value configured for the captive portal.	Integer (seconds)	Optional	0

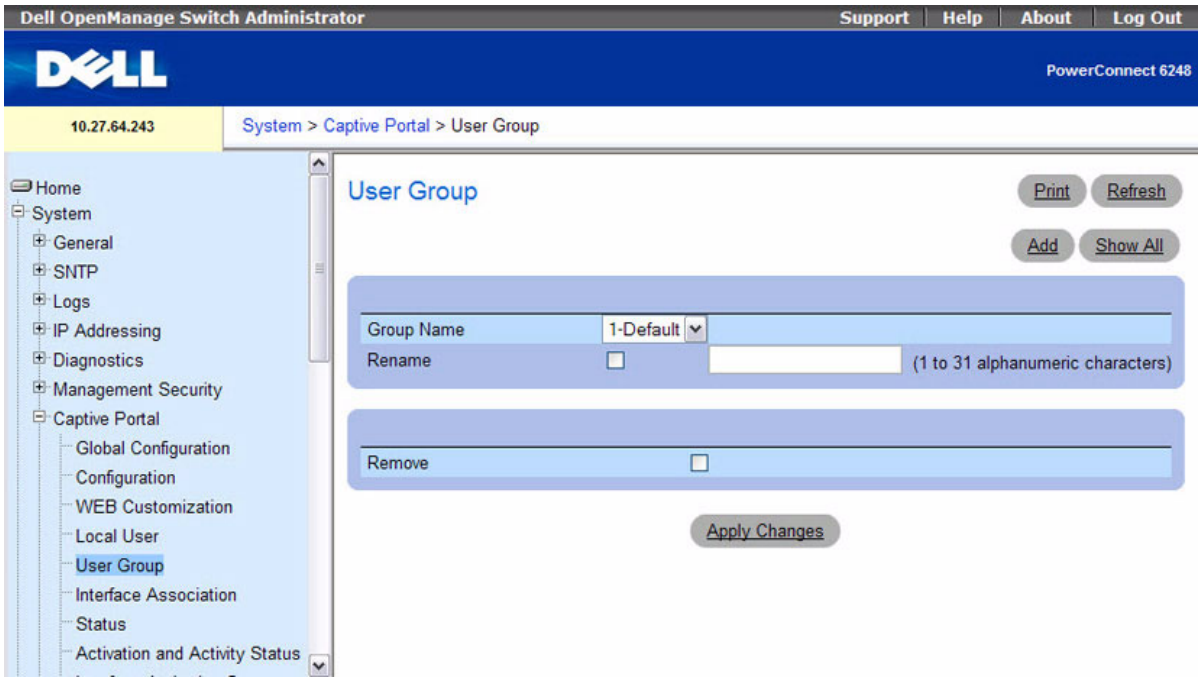
User Group

You can assign Local Users to User Groups that you create. If the Verification Mode is Local or RADIUS, you assign a User Group to a CP Configuration. All users who belong to the group are permitted to access the network through this portal. The User Group list is the same for all CP configurations on the switch.

To view and configure User Groups, click **System > Captive Portal > User Group**.

Downloaded from www.Manualslib.com manuals search engine

Figure 6-77. User Group



The **User Group** page contains the following fields:

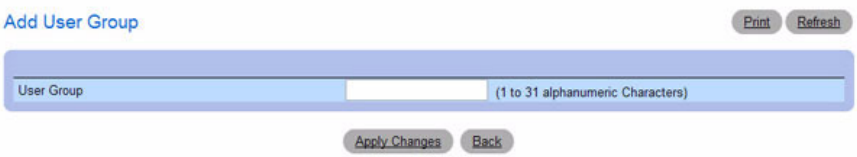
- **Group Name** — The menu contains the name of all of the groups configured on the system. The Default user group is configured by default. New users are assigned to the 1-Default user group by default. To delete a user group, select the name of the group from the Group Name menu, select the **Remove** option, and then click **Apply Changes**.
- **Rename** — To rename a Group Name, click the check box, type a new group name from 1 to 31 alphanumeric characters in the **Rename** field, then click **Apply Changes**.

Adding a User Group

1. Open the **User Group** page.
2. Click **Add**.

   The **Add Local User** page displays:

Figure 6-78. Add User Group



Downloaded from www.Manualslib.com manuals search engine

3. Enter a name for the new group.
4. Click **Apply Changes**.

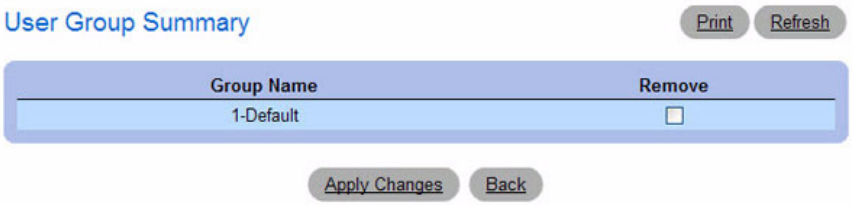
   The group is added, and the device is updated.

Displaying the User Group Page

1. Open the **User Group** page.
2. Click **Show All**.

   The **User Group Summary** page displays:

Figure 6-79. CP User Group Summary



3. To remove a configured group, select the **Remove** option in the appropriate row, and then click **Apply Changes**.

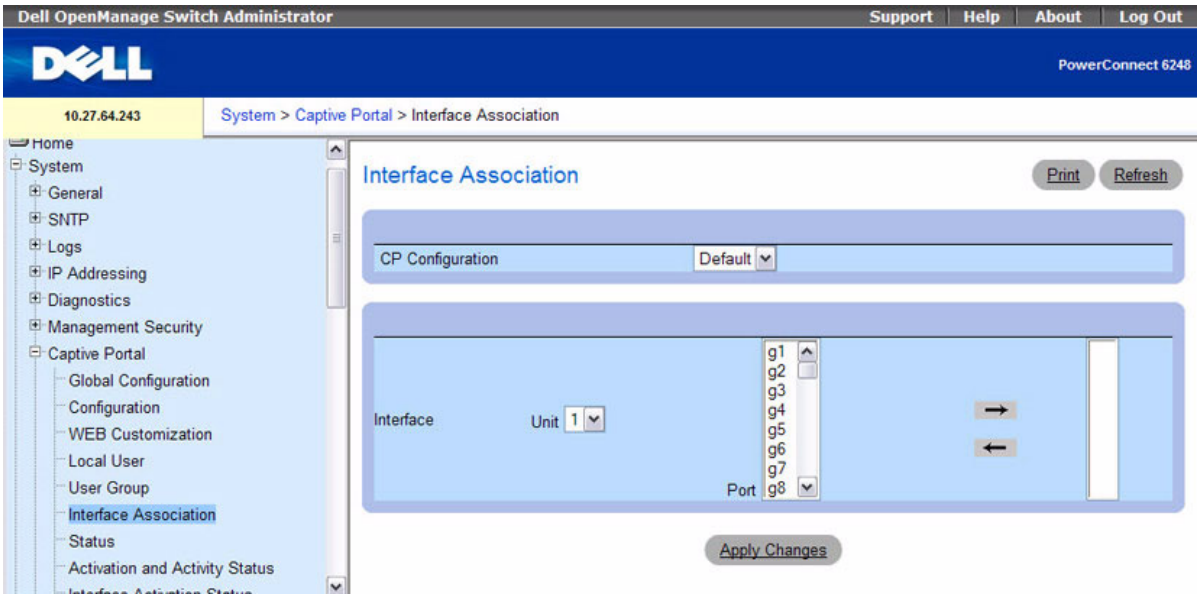
Interface Association

From the **Interface Association** page, you can associate a configured captive portal with specific interfaces. The captive portal feature only runs on the interfaces that you specify. A captive portal can have multiple interfaces associated with it, but an interface can be associated to only one CP at a time.

To view the **Interface Association** page, click **System > Captive Portal > Interface Association**.

Downloaded from www.Manualslib.com manuals search engine

Figure 6-80. CP Interface Association



The **Interface Association** page contains the following fields:

- **CP Configuration** — Lists the captive portals configured on the switch by number and name.
- **Interface List** — Lists the interfaces available on the switch that are not currently associated with a captive portal.

Use the following steps to associate one or more interfaces with a captive portal:

1. Select the desired captive portal from the **CP Configuration** list.
2. Select the interface or interfaces from the Interface list. To select more than one interface, hold **CTRL** and click multiple interfaces.
3. Click **Apply Changes**.

NOTE: When you associate an interface with a captive portal, the interface is removed from the Interface List. Each interface can be associated with only one captive portal at a time.

Use the following steps to remove an interface from the Associated Interfaces list for a captive portal:

1. Select the desired captive portal from the **CP Configuration** list.
2. In the Associated Interfaces field, select the interface or interfaces to remove. To select more than one interface, hold **CTRL** and click multiple interfaces.
3. Click **Delete**.
4. The interface is removed from the Associated Interface list and appears in the Interface List.

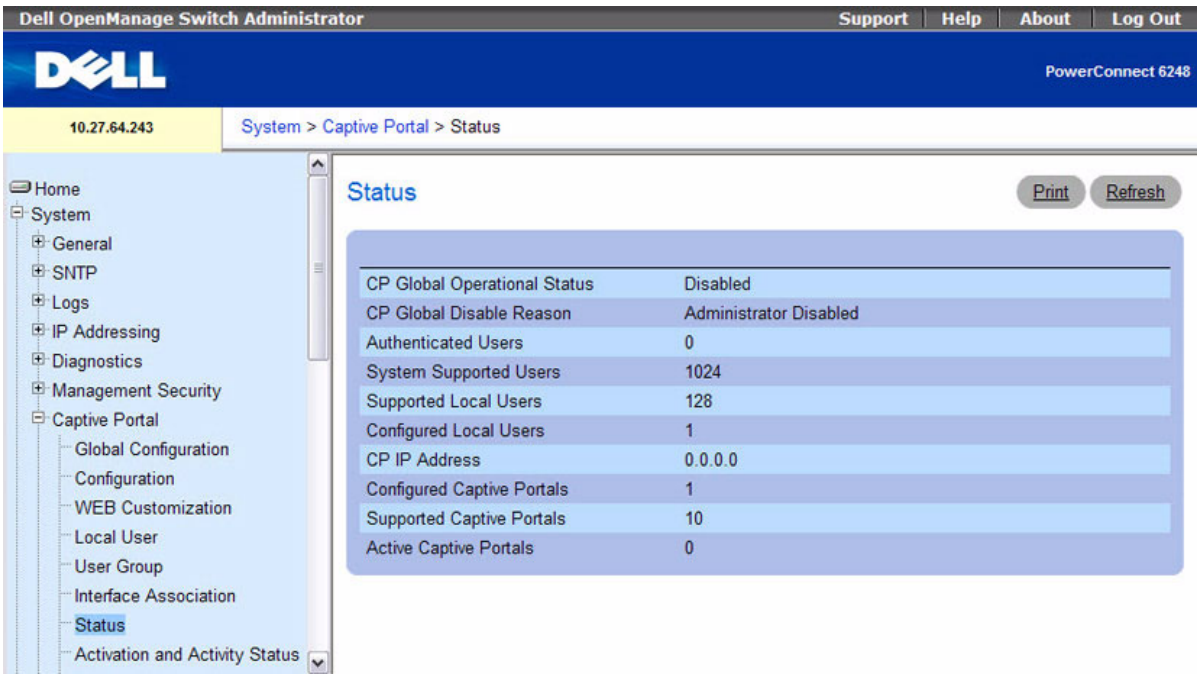
Downloaded from www.Manualslib.com manuals search engine

CP Status

The **CP Status** page contains a variety of information about the CP feature. From the **CP Status** page, you can access information about the CP activity and interfaces.

To view captive portal status information, click **System** > **Captive Portal** > **Status**.

Figure 6-81. CP Status



The **CP Status** page contains the following fields:

- **CP Global Operational Status** — Shows whether the CP feature is enabled.
- **CP Global Disable Reason** — Indicates the reason for the CP to be disabled, which can be one of the following:
  - None
  - Administratively Disabled
  - No IPv4 Address
  - Routing Enabled, but no IPv4 routing interface
- **Authenticated Users** — Shows the number of users currently authenticated to all captive portal instances on this switch.
- **System Supported Users** — Shows the number of authenticated users that the system can support.
- **Supported Local Users** — Shows the number of entries that the Local User database supports.
- **Configured Local Users** — Shows the number of entries configured as local Users.

Downloaded from www.Manualslib.com manuals search engine

- **CP IP Address** — Shows the captive portal IP address
- **Configured Captive Portals** — Shows the number of captive portals configured on the switch.
- **Supported Captive Portals** — Shows the number of supported captive portals in the system.
- **Active Captive Portals** — Shows the number of captive portal instances that are operationally enabled.

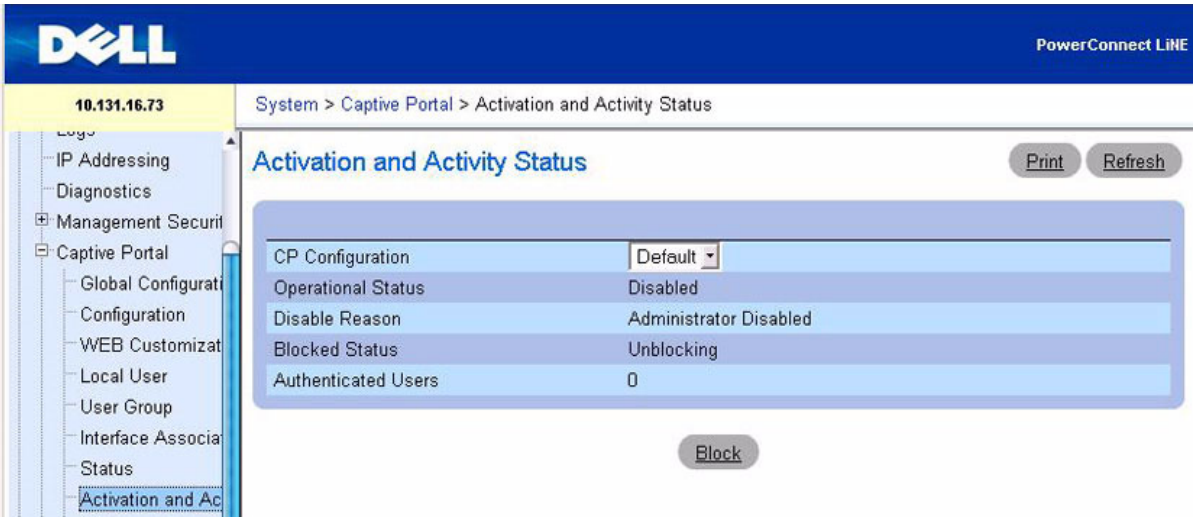
CP Activation and Activity Status

The **CP Activation and Activity Status** page provides information about each CP configured on the switch.

The **CP Activation and Activity Status** page has a drop-down menu that contains all captive portals configured on the switch. When you select a captive portal, the activation and activity status for that portal displays.

To view activation and activity information, click **System > Captive Portal > Activation and Activity Status**.

Figure 6-82. CP Activation and Activity Status



The **CP Activation and Activity Status** page contains the following fields:

- **CP Configuration** — Select the CP configuration with the information to view.
- **Operational Status** — Indicates whether the captive portal is enabled or disabled.
- **Disable Reason** — If the captive portal is disabled, then this field indicates the reason. The portal instance may be disabled for the following reasons:
  - None — CP is enabled.
  - Administrator Disabled
  - RADIUS Authentication mode enabled, but RADIUS server is not defined.
  - Not associated with any interfaces.

Downloaded from www.Manualslib.com manuals search engine

– The associated interfaces do not exist or do not support the CP capability.

- **Blocked Status** — Indicates whether authentication attempts to the captive portal are currently blocked.

  Use the Block and Unblock buttons to control the blocked status. If the CP is blocked, users cannot gain access to the network through the CP. Use this function to temporarily protect the network during unexpected events, such as denial of service attacks.

- **Authenticated Users** — Shows the number of users that successfully authenticated to this captive portal and are currently using the portal.

The following buttons are available on the CP Activation and Activity page:

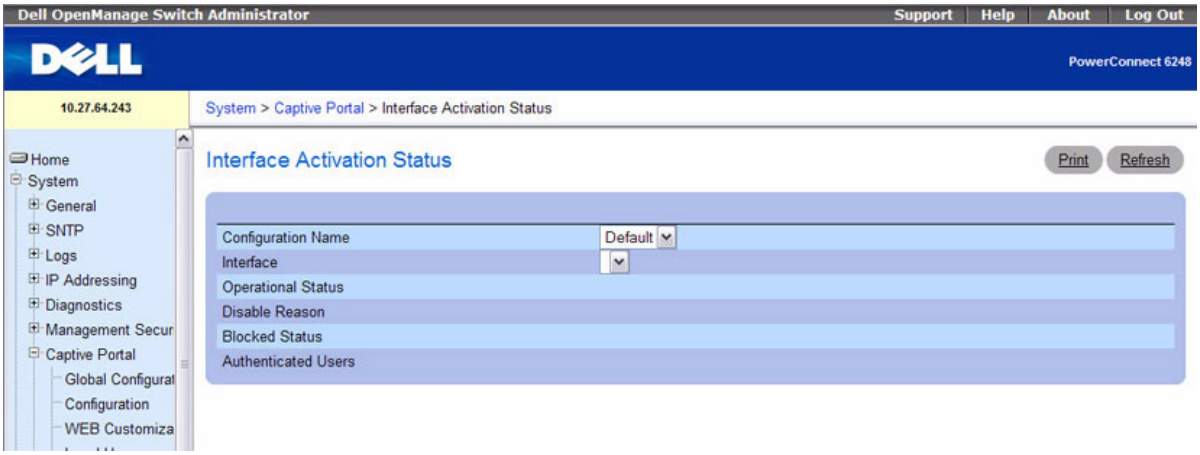
- **Block**—Click Block to prevent users from gaining access to the network through the selected captive portal.
- **Unblock**—If the Blocked Status of the selected captive portal is Blocked, click Unblock to allow access to the network through the captive portal.

Interface Activation Status

The **Interface Activation Status** page shows information for every interface assigned to a captive portal instance.

To view interface activation status information, click **System > Captive Portal > Interface Activation Status**.

Figure 6-83. Interface Activation Status



The **Interface Activation Status** page contains the following fields:

- **Configuration Name** — Select the CP configuration with the information to view.
- **Operational Status** — Shows whether the portal is active on the specified interface.

Downloaded from www.Manualslib.com manuals search engine

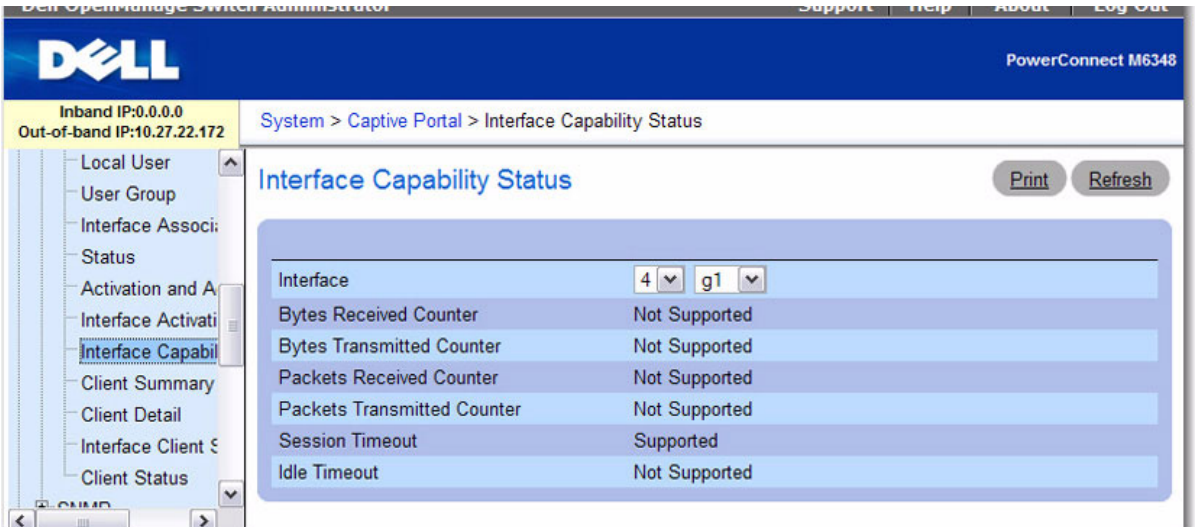
- **Disable Reason** — If the selected CP is disabled on this interface, this field indicates the reason, which can be one of the following:
  - Interface Not Attached
  - Disabled by Administrator
- **Blocked Status** — Indicates whether the captive portal is temporarily blocked for authentications.
- **Authenticated Users** — Displays the number of authenticated users using the captive portal instance on this interface.

Interface Capability Status

The **Interface Capability Status** page contains information about interfaces that can have CPs associated with them. The page also contains status information for various capabilities. Specifically, this page indicates what services are provided through the CP to clients connected on this interface. The list of services is determined by the interface capabilities.

To view interface activation status information, click **System > Captive Portal > Interface Capability Status**.

Figure 6-84. Interface Capability Status



The **Interface Capability Status** page contains the following fields:

- **Interface** — Select the interface with the information to view.
- **Bytes Received Counter** — Shows whether the interface supports displaying the number of bytes received from each client.
- **Bytes Transmitted Counter** — Shows whether the interface supports displaying the number of bytes transmitted to each client.

Downloaded from www.Manualslib.com manuals search engine

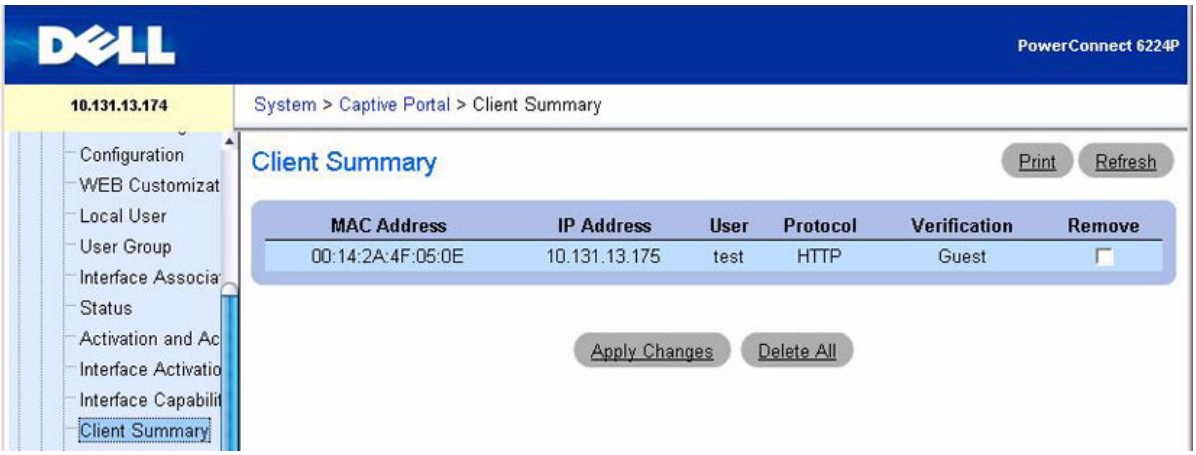
- **Packets Received Counter** — Shows whether the interface supports displaying the number of packets received from each client.
- **Packets Transmitted Counter** — Shows whether the interface supports displaying the number of packets transmitted to each client.
- **Session Timeout** — Shows whether the interface supports client session timeout. This attribute is supported on all interfaces.
- **Idle Timeout** — Shows whether the interface supports a timeout when the user does not send or receive any traffic.

Client Summary

Use the **Client Summary** page to view summary information about all authenticated clients that are connected through the captive portal. From this page, you can manually force the captive portal to disconnect one or more authenticated clients. The list of clients is sorted by client MAC address.

To view information about the clients connected to the switch through the captive portal, click **System > Captive Portal > Client Connection Status**.

Figure 6-85. Client Summary



The **Client Summary** page contains the following fields:

- **MAC Address** — Identifies the MAC address of the client (if applicable).
- **IP Address** — Identifies the IP address of the client (if applicable).
- **User** — Displays the user name (or Guest ID) of the connected client.
- **Protocol** — Shows the current connection protocol, which is either HTTP or HTTPS.
- **Verification** — Shows the current account type, which is Guest, Local, or RADIUS.

To force the captive portal to disconnect an authenticated client, select the **Remove** check box next to the client MAC address and click **Apply Changes**. To disconnect all clients from all captive portals, click **Delete All.**

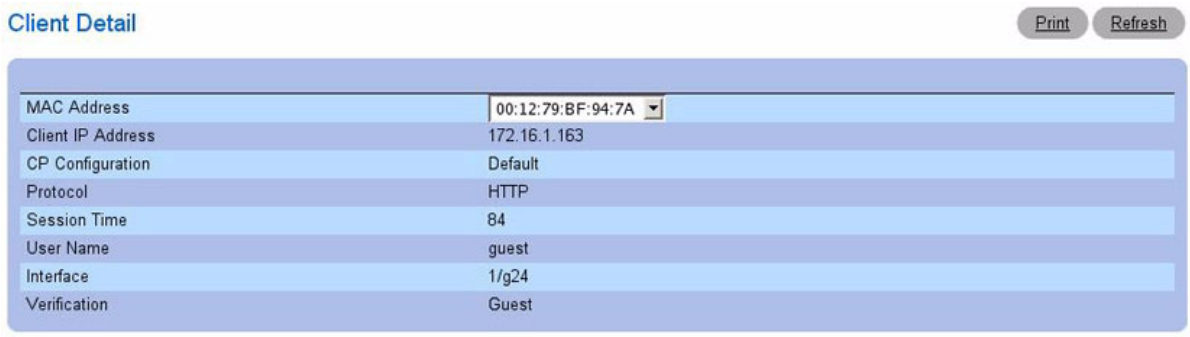
Downloaded from www.Manualslib.com manuals search engine

Client Detail

The **Client Detail** page shows detailed information about each client connected to the network through a captive portal.

To view detailed information about the clients connected to the switch through the captive portal, click **System > Captive Portal > Client Detail**.

Figure 6-86. Client Detail



The **Client Detail** page contains the following fields:

- **MAC Address —** The menu lists each associated client by MAC address. To view status information for a different client, select its MAC address from the list.
- **Client IP Address** — Identifies the IP address of the client (if applicable).
- **CP Configuration** — Identifies the CP configuration the client is using.
- **Protocol** — Shows the current connection protocol, which is either HTTP or HTTPS.
- **Session Time** — Shows the amount of time that has passed since the client was authorized.
- **User Name** — Displays the user name (or Guest ID) of the connected client.
- **Interface** — Identifies the interface the client is using.
- **Verification** — Shows the current account type, which is Guest, Local, or RADIUS.

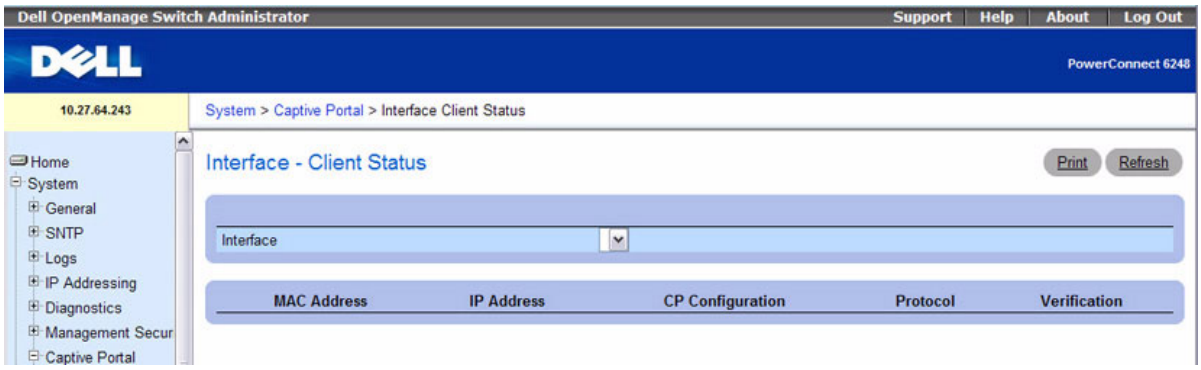
CP Interface Client Status

Use the **Interface Client Status** page to view clients that are authenticated to a specific interface.

To view statistical information for clients connected to the switch through the captive portal, click **System > Captive Portal > Interface Client Status**.

Downloaded from www.Manualslib.com manuals search engine

Figure 6-87. Interface - Client Status



The **Interface Client Status** page contains the following fields:

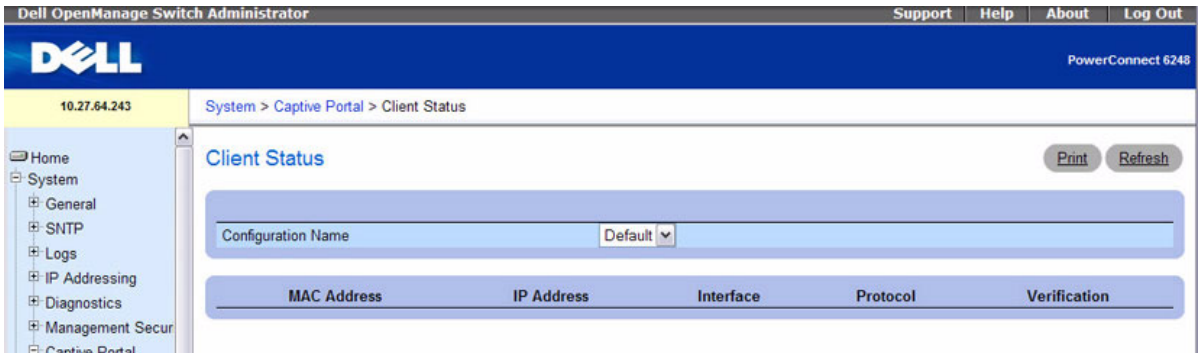
- **Interface** — The drop-down menu lists each interface on the switch. To view information about the clients connected to a CP on this interface, select it from the list.
- **MAC Address** — Identifies the MAC address of the client.
- **IP Address** — Identifies the IP address of the client.
- **CP Configuration** — Identifies the captive portal the client used to access the network.
- **Protocol** — Shows the current connection protocol, which is either HTTP or HTTPS.
- **Verification** — Shows the current account type, which is Guest, Local, or RADIUS.

CP Client Status

Use the **Client Status** page to view clients that are authenticated to a specific CP configuration.

To view information about clients connected to the switch through the a specific captive portal, click **System > Captive Portal > Client Status**.

Figure 6-88. CP - Client Status



The **CP - Client Status** page contains the following fields:

Downloaded from www.Manualslib.com manuals search engine

- **Configuration Name** — The drop-down menu lists each CP configured on the switch. To view information about the clients connected to the CP configuration, select the CP configuration name from the list.
- **MAC Address** — Identifies the MAC address of the client.
- **IP Address** — Identifies the IP address of the client.
- **Interface** — Identifies the interface the client used to access the network.
- **Protocol** — Shows the current connection protocol, which is either HTTP or HTTPS.
- **Verification** — Shows the current account type, which is Guest, Local, or RADIUS.

Defining SNMP Parameters

Simple Network Management Protocol (SNMP) provides a method for managing network devices. The device supports SNMP version 1, SNMP version 2, and SNMP version 3.

Note: By default, SNMPv2 is automatically enabled on the device. To enable SNMPv3, a local engine ID must be defined for the device. The local engineID is by default set to the switch MAC address. This local engineID must be defined so that it is unique within the network. For information on how to configure the local engine ID, see "SNMP Global Parameters."

SNMP v1 and v2

The SNMP agent maintains a list of variables, which are used to manage the device. The variables are defined in the Management Information Base (MIB). The MIB presents the variables controlled by the agent. The SNMP agent defines the MIB specification format, as well as the format used to access the information over the network. Access rights to the SNMP agent are controlled by access strings.

SNMP v3

SNMP v3 also applies access control and a new traps mechanism to SNMPv1 and SNMPv2 PDUs. In addition, the User Security Model (USM) is defined for SNMPv3 and includes:

- **Authentication** — Provides data integrity and data origin authentication.
- **Privacy** — Protects against disclosure of message content. Cipher-Bock-Chaining (CBC) is used for encryption. Either authentication is enabled on an SNMP message, or both authentication and privacy are enabled on an SNMP message. However privacy cannot be enabled without authentication.
- **Timeliness** — Protects against message delay or message redundancy. The SNMP agent compares incoming message to the message time information.
- **Key Management** — Defines key generation, key updates, and key use.

The device supports SNMP notification filters based on Object IDs (OID). OIDs are used by the system to manage device features. SNMP v3 supports the following features:

- Security
- Feature Access Control

Downloaded from www.Manualslib.com manuals search engine

- Traps

Authentication or Privacy Keys are modified in the SNMPv3 User Security Model (USM).

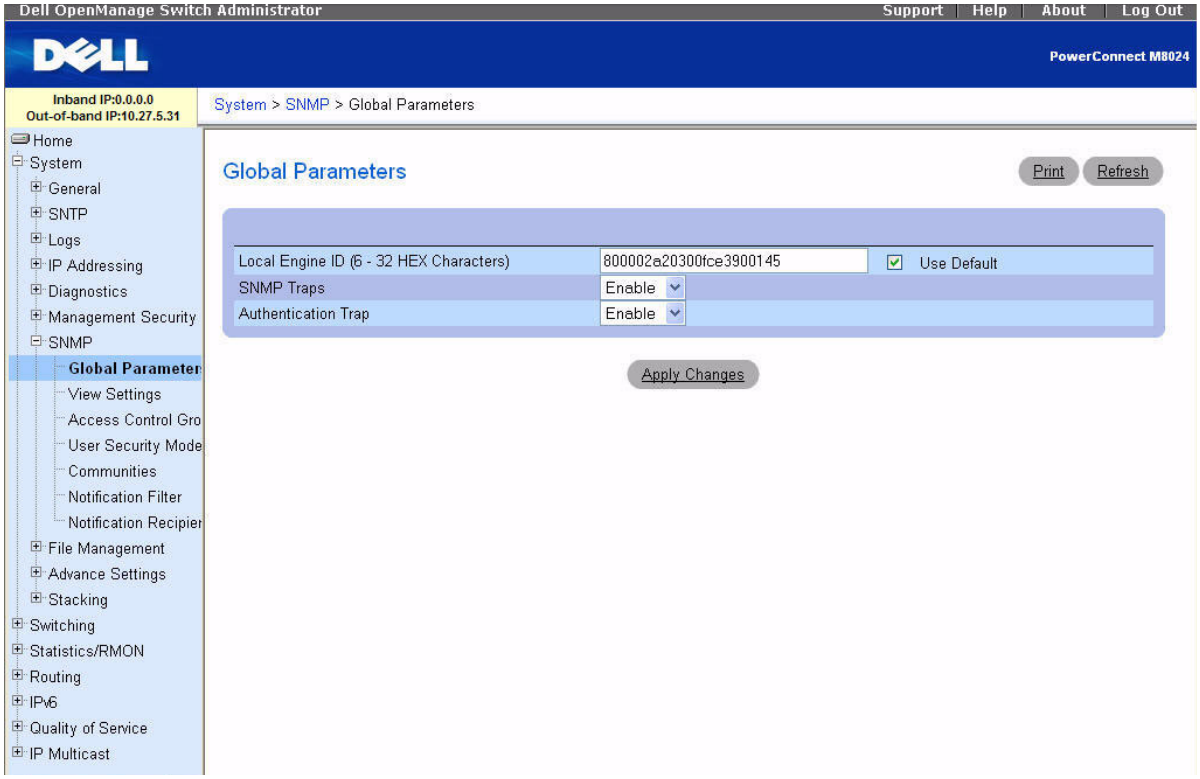
Use the **SNMP** page to define SNMP parameters. To display the **SNMP** page, click **System > SNMP** in the tree view.

SNMP Global Parameters

Use the **Global Parameters** page to enable SNMP and Authentication notifications.

To display the **Global Parameters** page, click **System > SNMP > Global Parameters** in the tree view.

Figure 6-89. Global Parameters



The **Global Parameters** page contains the following parameters:

- **Local Engine ID (6 – 32 hexadecimal characters) —** Sets local SNMP engine ID.
- **Use Default** — Configures the device to use the default SNMP EngineID.
- **SNMP Traps —** Enables or disables the device sending SNMP notifications.
- **Authentication Trap —** Enables or disables the device sending SNMP traps when authentication fails.

Setting Local SNMP Engine ID

1. Open the **Global Parameters** page.

Downloaded from www.Manualslib.com manuals search engine

2. Type desired hexadecimal ID into the **Local Engine ID** field.
3. Click **Apply Changes**.

   The new Local Engine ID is set, and the device is updated.

Using Default SNMP Engine ID

1. Open the **Global Parameters** page.
2. Click the **Use Default** check box.
3. Click **Apply Changes**.

   The default SNMP engine ID, based on the MAC address, is created and the device is updated.

Enabling SNMP Traps

1. Open the **Global Parameters** page.
2. Select **Enable** in the **SNMP Traps** field.
3. Click **Apply Changes**.

   SNMP notifications are enabled, and the device is updated.

Enabling Authentication Trap

1. Open the **Global Parameters** page.
2. Select **Enable** in the **Authentication trap** field.
3. Click **Apply Changes**.

   Authentication notifications are enabled, and the device is updated.

Enabling SNMP Notifications Using CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- SNMP Commands.

SNMP View Settings

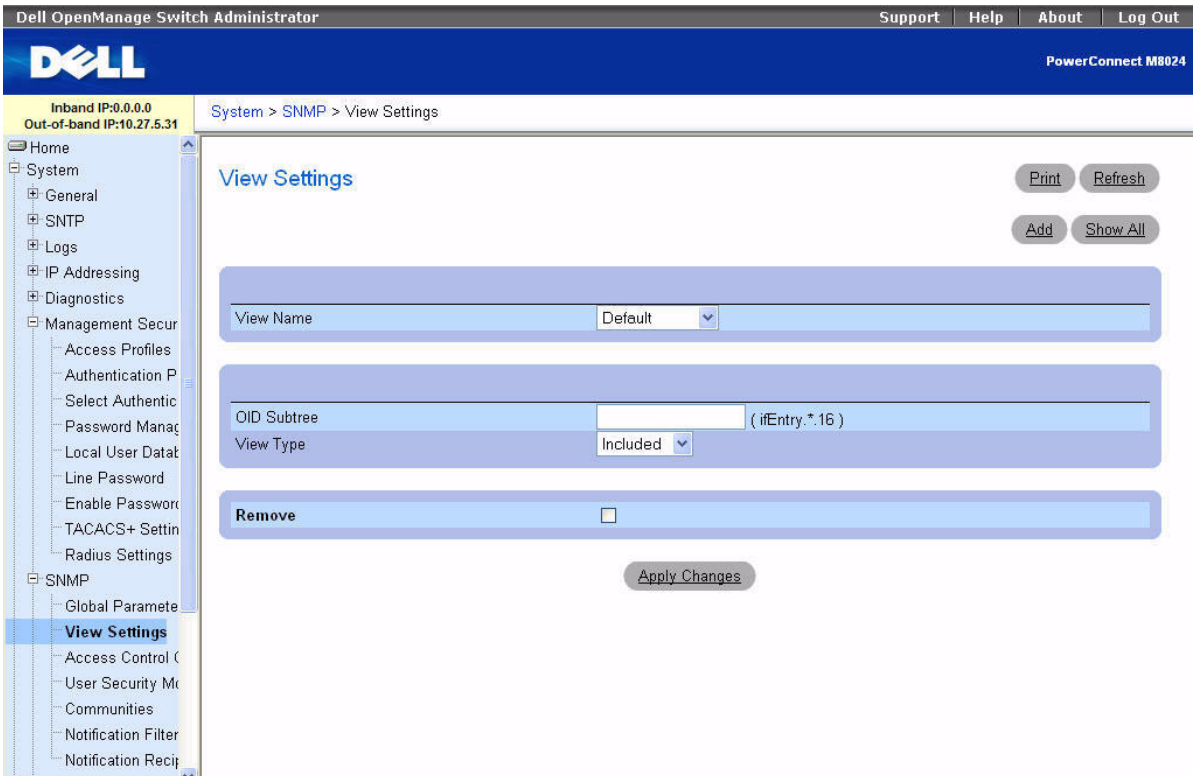
Use this page to create views that define which features of the device are accessible, and which are blocked. You can create a view that includes or excludes OIDs corresponding to interfaces.

Use the **SNMP View Settings** page to define SNMP views.

To display the **SNMP View Settings** page, click **System > SNMP > View Settings** in the tree view.

Downloaded from www.Manualslib.com manuals search engine

Figure 6-90. SNMP View Settings



The **SNMP View Settings** page contains the following fields:

- **View Name** — Contains a list of user-defined views. A view name can contain a maximum of 30 alphanumeric characters.
- **OID Subtree** — Specifies a valid SNMP OID string that can include meta characters like *.
- **View Type —** Specifies whether the objectIDs in the view are included or excluded.
- **Remove —** Check to remove displayed view type.

Adding a View

1. Open the **SNMP View Settings** page.
2. Click **Add**.

   The **Add View** page displays:

Downloaded from www.Manualslib.com manuals search engine

Figure 6-91. Add View

3. Define the relevant fields.
4. Click **Apply Changes**.

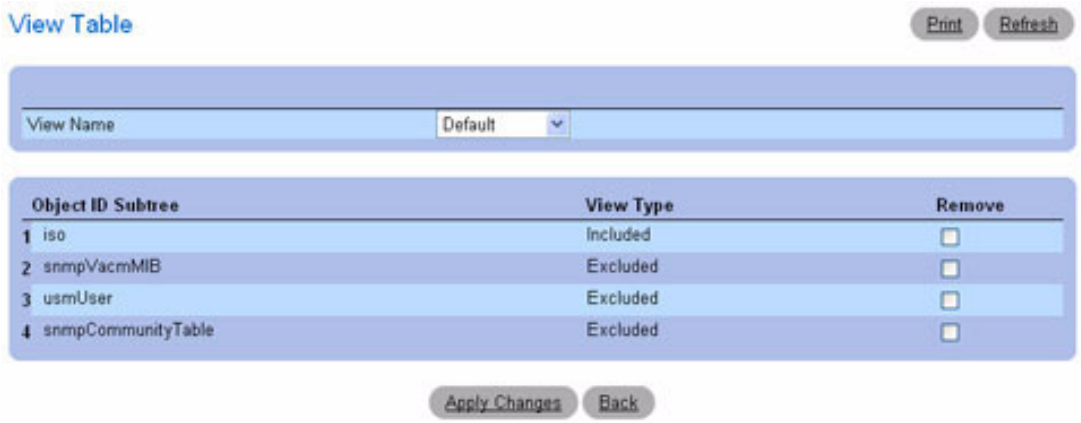
   The SNMP view is added, and the device is updated.

Displaying the View Table

1. Open the **SNMP View Settings** page.
2. Click **Show All**.

   The **View Table** page displays:

Figure 6-92. View Table



Downloaded from www.Manualslib.com manuals search engine

Removing SNMP Views

1. Open the **SNMP View Settings** page.
2. Click **Show All**.

   The **View Table** page displays.
3. Select an SNMP view.
4. Check the **Remove** check box.
5. Click **Apply Changes**.

   The SNMP view is removed, and the device is updated.

Defining SNMP Views Using CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- SNMP Commands.

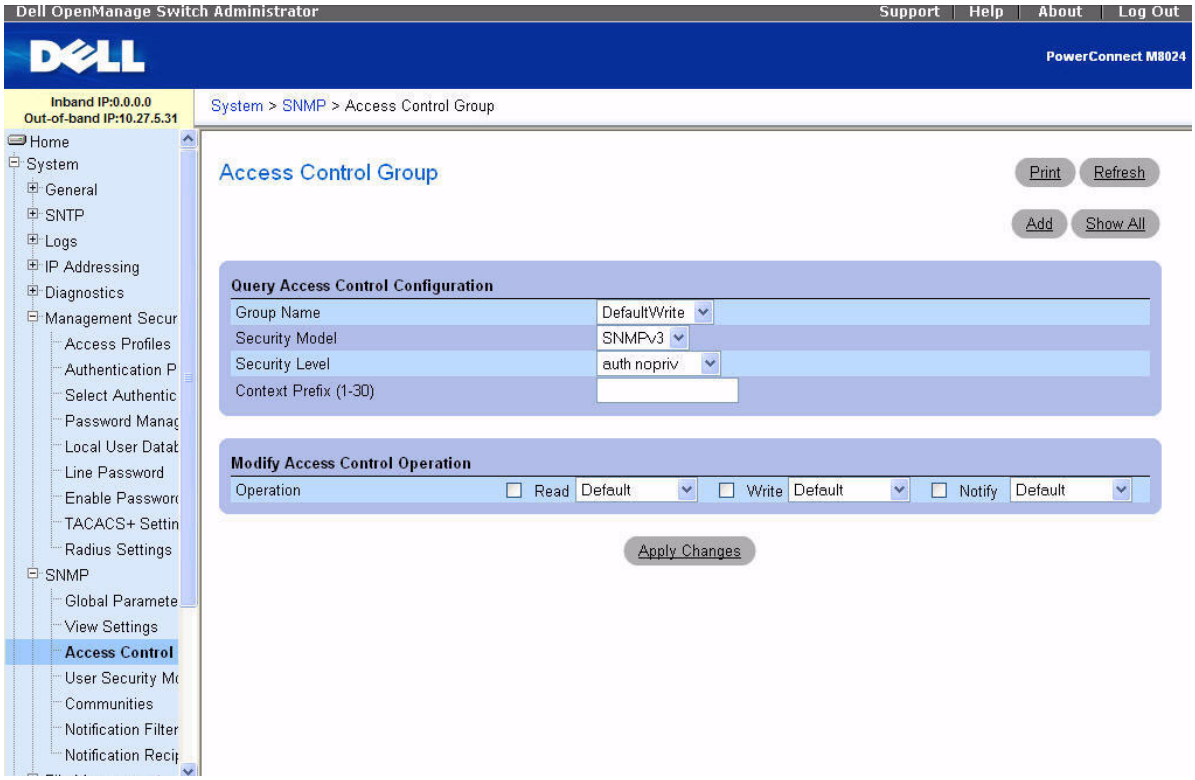
Access Control Group

Use the **Access Control Group** page to view information for creating SNMP groups, and to assign SNMP access privileges. Groups allow network managers to assign access rights to specific device features or features aspects.

To display the **Access Control Group** page, click **System** > **SNMP** > **Access Control** in the tree view.

Downloaded from www.Manualslib.com manuals search engine

Figure 6-93. Access Control Group



The **Access Control Group** page contains the following fields:

- **Group Name** — Contains a list of user-defined groups to which access control rules are applied. A group name can contain a maximum of 30 alphanumeric characters.
- **Security Model —** Defines the SNMP version attached to the group. The possible field values are:
  - **SNMPv1** — SNMPv1 is defined for the group.
  - **SNMPv2** — SNMPv2 is defined for the group.
  - **SNMPv3** — SNMPv3 User Security Model (USM) is defined for the group.
- **Security Level** — The security level attached to the group. Security levels apply to SNMPv3 groups only. The possible field values are:
  - **noauth no priv** — Neither Authentication nor Privacy security levels are assigned to the group.
  - **auth nopriv** — Authenticates SNMP messages without encrypting them.
  - **auth priv** — Authenticates SNMP messages and encrypts them.
- **Context Prefix (1–30)** — This field permits the user to specify the context name by entering the first 1 to 30 characters of the context name.
- **Operation** — Defines group access rights. The possible field values are:

Downloaded from www.Manualslib.com manuals search engine

– **Read** — Select a view that restricts management access to viewing the contents of the agent. If no view is selected, all objects except the community-table, SNMPv3 user and access tables can be viewed.

– **Write** — Select a view that permits management read-write access to the contents of the agent.

– **Notify** — Select a view that permits sending SNMP traps or informs.

Adding SNMP Groups

1. Open the **Access Control Configuration** page.
2. Click **Add**.

   The **Add an Access Control Configuration** page displays:

Figure 6-94. Add an Access Control Configuration

3. Define the fields as needed.
4. Click **Apply Changes**.

   The group is added, and the device is updated.

Displaying the Access Table

1. Open the **Access Control Configuration** page.
2. Click **Show All**.

   The **Access Table** page displays:

Downloaded from www.Manualslib.com manuals search engine

Figure 6-95. Access Table

Access Table

Print Refresh

	Group Name	Context Prefix	SNMP Version	Security Level	Read	Write	Notify	Remove
1	DefaultRead		SNMPV1	NoAuth NoPriv	Default		Default	☐
2	DefaultRead		SNMPV2	NoAuth NoPriv	Default		Default	☐
3	DefaultSuper		SNMPV1	NoAuth NoPriv	DefaultSuper	DefaultSuper	DefaultSuper	☐
4	DefaultSuper		SNMPV2	NoAuth NoPriv	DefaultSuper	DefaultSuper	DefaultSuper	☐
5	DefaultWrite		SNMPV1	NoAuth NoPriv	Default	Default	Default	☐
6	DefaultWrite		SNMPV2	NoAuth NoPriv	Default	Default	Default	☐

Removing a Group

1. Open the **Access Control Configuration** page.
2. Click **Show All**.

   The **Access Table** opens.
3. Select a group.
4. Check **Remove**.
5. Click **Apply Changes**.

   The group is removed, and the device is updated.

Defining SNMP Access Control Using CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- SNMP Commands.

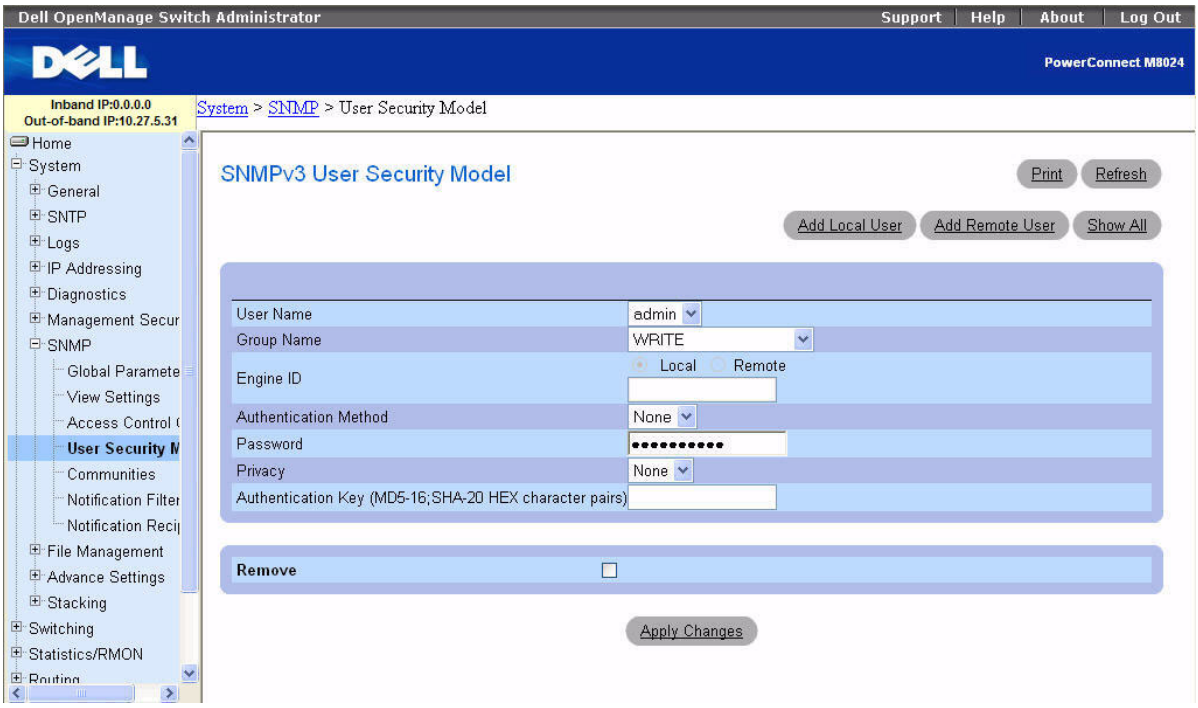
SNMPv3 User Security Model (USM)

Use the **SNMPv3 User Security Model (USM)** page to assign system users to SNMP groups and to define the user authentication method.

To display the **SNMPv3 User Security Model (USM)** page, click **System > SNMP > User Security Model** in the tree view.

Downloaded from www.Manualslib.com manuals search engine

Figure 6-96. SNMPv3 User Security Model (USM)



The **SNMPv3 User Security Model (USM)** page contains the following fields:

- **User Name** — Contains a list of user-defined user names.
- **Group Name** — Contains a list of user-defined SNMP groups. SNMP groups are defined in the **Access Control Group** page.
- **Engine ID** — Selects whether the selected user is associated to a local or to a specified remote SNMPv3 enabled device.
  - Remote Engine ID — Indicates that the user is configured on a remote SNMPv3 enabled device.
- **Authentication Method** — Specifies the authentication method used to authenticate users. The possible field values are:
  - **None** — No user authentication is used.
  - **MD5 —** Users are authenticated using the HMAC-MD5-96 authentication level. The user should specify a password.
  - **SHA —** Users are authenticated using the HMAC-SHA-96 authentication level. The user should enter a password.
- **Password** — Modifies the user defined password for the group. Passwords can contain a maximum of 32 characters. Passwords are defined only if the authentication method is MD5 or SHA Password. You define the password on the **Add Local User** page.

Downloaded from www.Manualslib.com manuals search engine

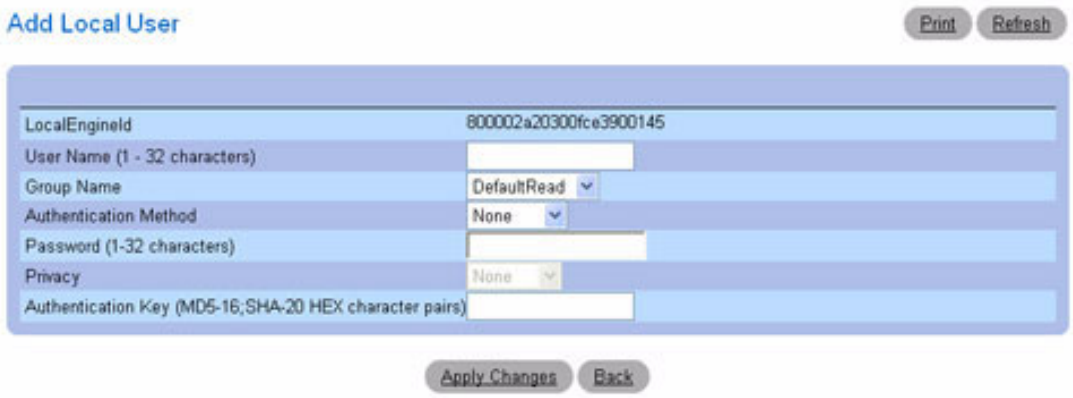
- **Privacy** — Specifies whether or not the authentication key is to be used. Choose one of the following values:
  - **None —** Do not use an authentication key.
  - **des** — Use a CBC-DES Symmetric Encryption Password for the authentication key.
  - **des-key** — Use an HMAC-MD5-96 Authentication Pre-generated key.
- **Authentication Key(MD5-16; SHA-20 HEX character pairs) —** Specify the authentication key. An authentication key is defined only if the authentication method is MD5 or SHA.
- **Remove** — Removes the specified user from the specified group when checked.

Adding SNMPv3 Local Users to a Group

1. Open the **SNMPv3 User Security Model** page.
2. Click **Add Local User**.

   The **Add Local User** page displays:

Figure 6-97. Add Local User



3. Define the relevant fields.
4. Click **Apply Changes**.
5. The user is added to the group, and the device is updated.

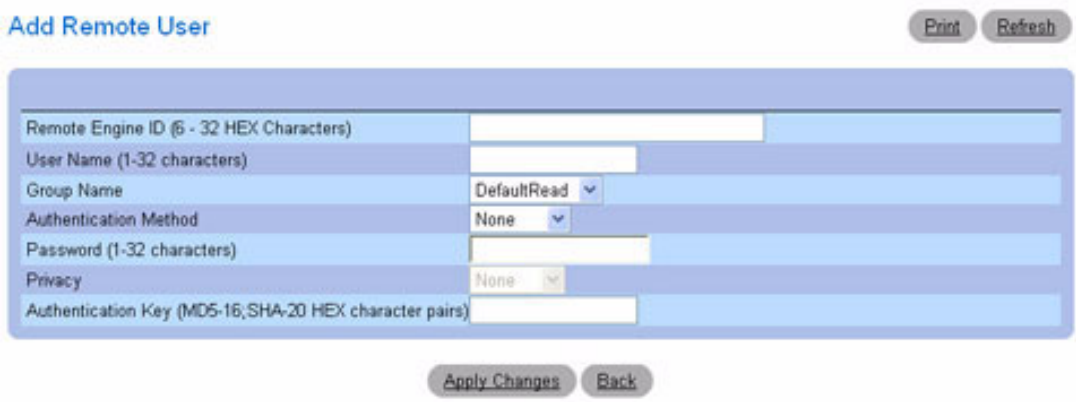
Adding SNMPv3 Remote Users to a Group

1. Open the **SNMPv3 User Security Model** page.
2. Click **Add Remote User**.

   The **Add Remote User** page displays:

Downloaded from www.Manualslib.com manuals search engine

Figure 6-98. Add Remote User



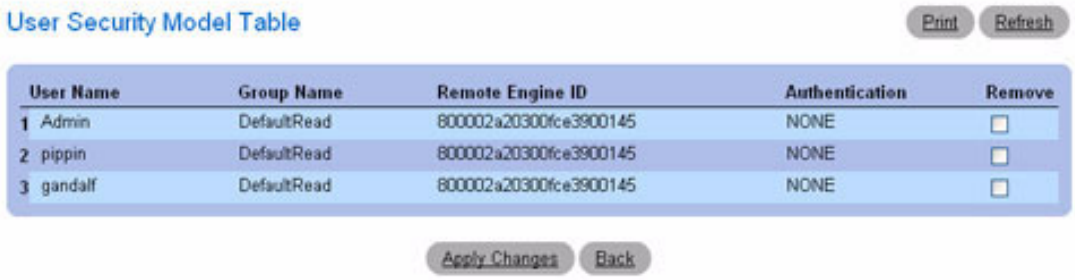
3. Define the relevant fields.
4. Click **Apply Changes**.
5. The user is added to the group, and the device is updated.

Viewing the User Security Model Table

1. Open the **SNMPv3 User Security Model (USM)** page.
2. Click **Show All**.

   The **User Security Model Table** displays:

Figure 6-99. User Security Model Table



Downloaded from www.Manualslib.com manuals search engine

Removing a User Security Model Table Entry

1. Open the **User Security Model** page.
2. Click **Show All**.

   The **User Security Model Table** page displays.
3. Select an entry.
4. Check the **Remove** check box.
5. Click **Apply Changes**.

   The entry is removed, and the device is updated.

Defining SNMP Users Using CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- SNMP Commands.

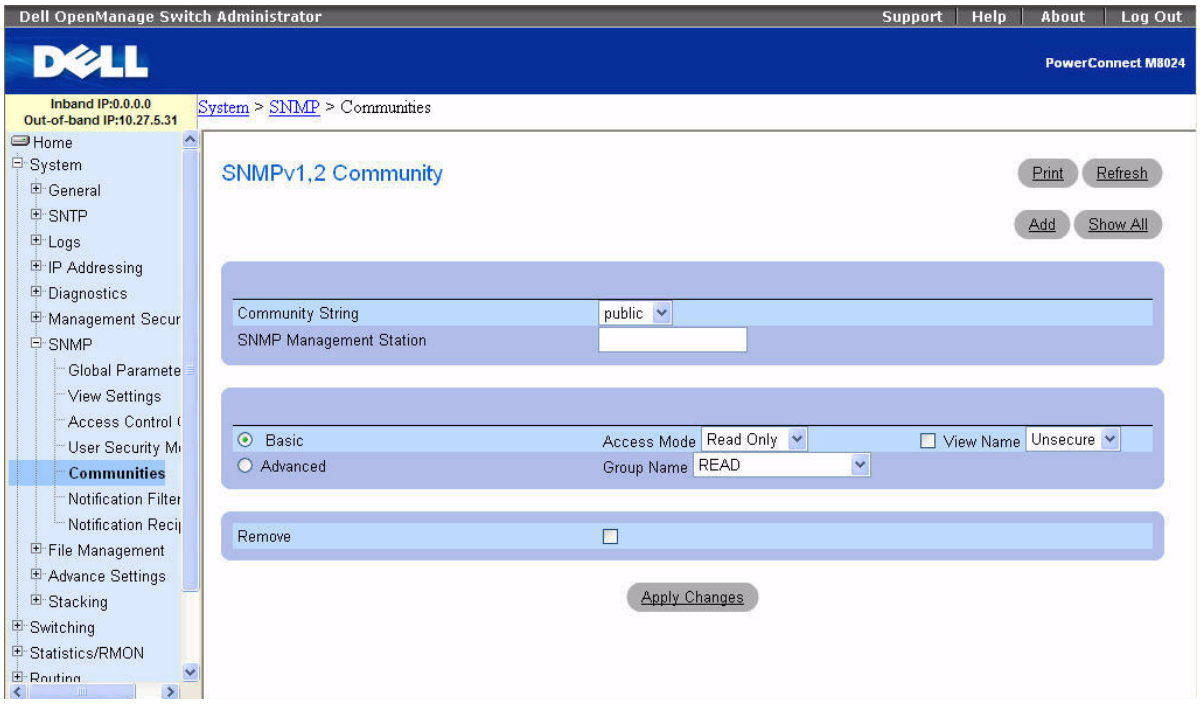
Communities

Access rights are managed by defining communities on the **SNMPv1, 2 Community** page. When the community names are changed, access rights are also changed. SNMP Communities are defined only for SNMP v1 and SNMP v2.

To display the **SNMPv1, 2 Community** page, click **System** > **SNMP** > **Communities** in the tree view.

Downloaded from www.Manualslib.com manuals search engine

Figure 6-100. SNMPv1, 2 Community



The **SNMPv1, 2 Community** page contains the following fields:

- **Community String —** Contains a list of user-defined community strings that act as a password and are used to authenticate the SNMP management station to the device. A community string can contain a maximum of 20 characters.
- **SNMP Management Station** — Contains a list of management station IP address for which community strings have been defined.
- **Basic** — Enables SNMP Basic mode for the selected community. The possible field values are:
  - **Access Mode** — Defines the access rights of the community. The possible field values are:
    - **Read-Only** — Community has read only access to the MIB objects configured in the view.
    - **Read-Write** — Community has read/modify access to the MIB objects configured in the view.
    - **Super User** — Community has read/modify access to all MIB objects.
  - **View Name —** Contains a list of user-defined SNMP views.
- **Advanced** — Contains a list of user-defined groups. When SNMP Advanced mode is selected, the SNMP access control rules comprising the group are enabled for the selected community. The Advanced mode also enables SNMP groups for specific SNMP communities. The SNMP Advanced mode is defined only with SNMPv3.
- **Remove** — When checked, removes a community.

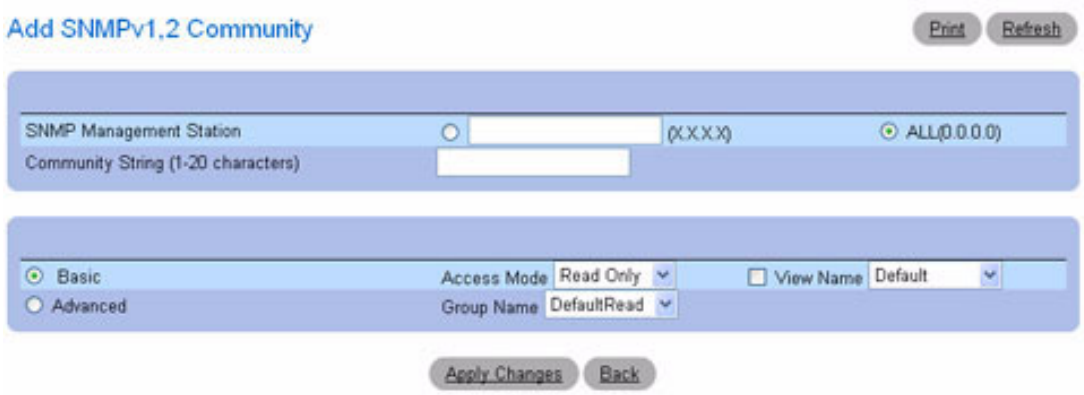
Downloaded from www.Manualslib.com manuals search engine

Adding a New Community

1. Open the **SNMPv1, 2 Community** page.
2. Click **Add**.

   The **Add SNMPv1,2 Community** page displays:

Figure 6-101. Add SNMPv1,2 Community



3. Complete the relevant fields.

   In addition to the fields in the **SNMPv1, 2 Community** page, the **Add SNMPv1,2 Community** page contains the **All (0.0.0.0)** field, which indicates that the community can be used from any management station.
4. Click **Apply Changes**.

   The new community is saved, and the device is updated.

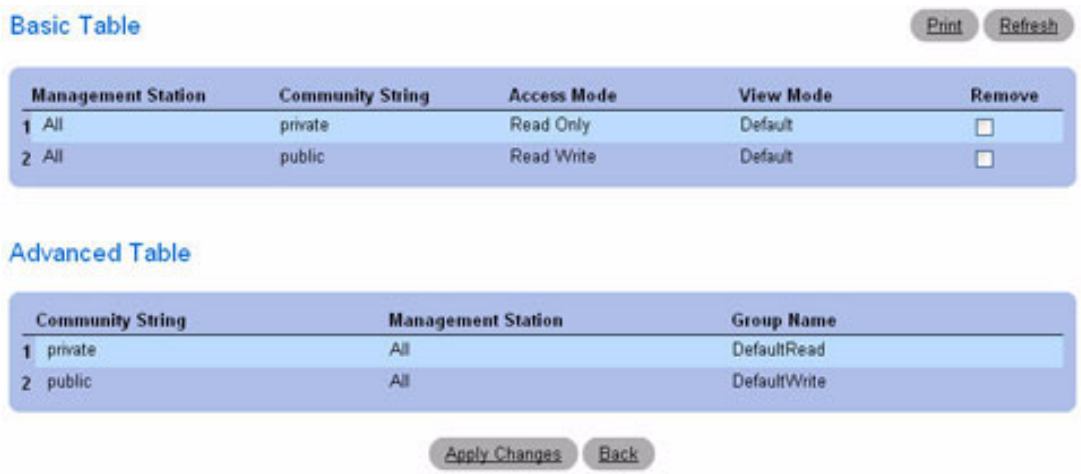
Displaying Communities

1. Open the **SNMPv1, 2 Community** page.
2. Click **Show All**.

   The **Basic and Advanced Table** page displays.

Downloaded from www.Manualslib.com manuals search engine

Figure 6-102. Basic and Advanced Table



Removing Communities

1. Open the **SNMPv1, 2 Community** page.
2. Click **Show All**.

   The **Basic and Advanced Table** page displays.
3. Select a community and check the **Remove** check box.
4. Click **Apply Changes**.

   The community entry is removed, and the device is updated.

Configuring Communities Using CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- SNMP Commands.

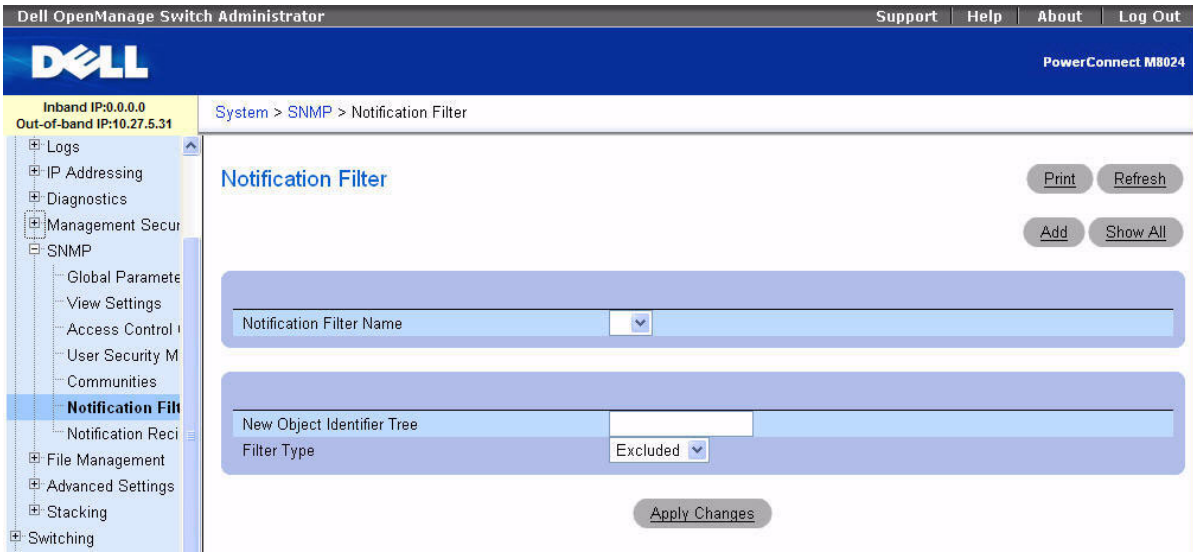
Notification Filter

Use the **Notification Filter** page to set filtering traps based on OIDs. Each OID is linked to a device feature or a feature aspect. The **Notification Filter** page also allows you to filter notifications.

To display the **Notification Filter** page, click **System** > **SNMP** > **Notification Filters** in the tree view.

Downloaded from www.Manualslib.com manuals search engine

Figure 6-103. Notification Filter



The **Notification Filter** page contains the following fields:

- **Notification Filter Name —** Contains a list of user-defined notification filters. A notification filter name can contain a maximum of 30 characters.
- **New Object Identifier Tree —** Displays the OID configured for the selected filter. This field can be edited.
- **Filter Type** — Indicates whether informs or traps are sent regarding the OID to the trap recipients.
  - **Excluded —** Restricts sending OID traps or informs.
  - **Included —** Sends OID traps or informs.

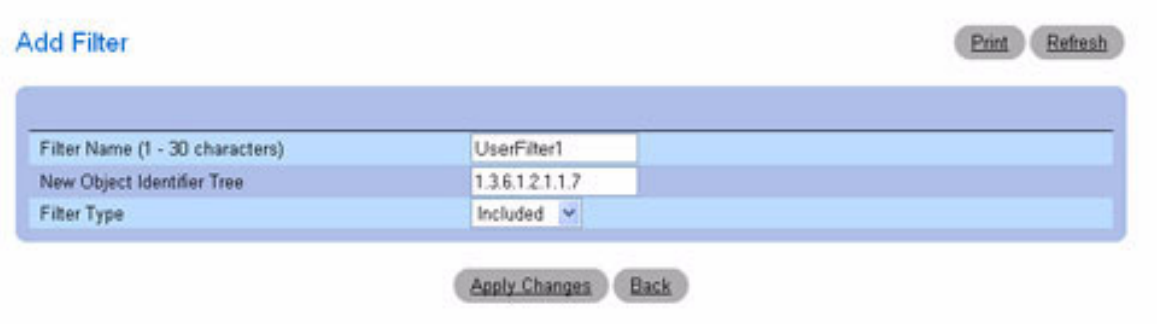
Adding SNMP Filters

1. Open the **Notification Filter** page.
2. Click **Add**.

   The **Add Filter** page displays:

Downloaded from www.Manualslib.com manuals search engine

Figure 6-104. Add Filter



3. Define the relevant fields.
4. Click **Apply Changes**.

   The new filter is added, and the device is updated.

Displaying the Filter Table

1. Open the **Notification Filter** page.
2. Click **Show All**.

   The **Filter Table** page appears, which displays all of the filters configured for the selected filter name:

Figure 6-105. Show Notification

Removing a Filter

1. Open the **Notification Filter** page.
2. Click **Show All**.

   The **Show Notification** page displays.
3. Select the **Filter Table** entry.
4. Check **Remove**.

   The filter entry is removed, and the device is updated.

Downloaded from www.Manualslib.com manuals search engine

Configuring Notification Filters Using CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- SNMP Commands.

Notification Recipients

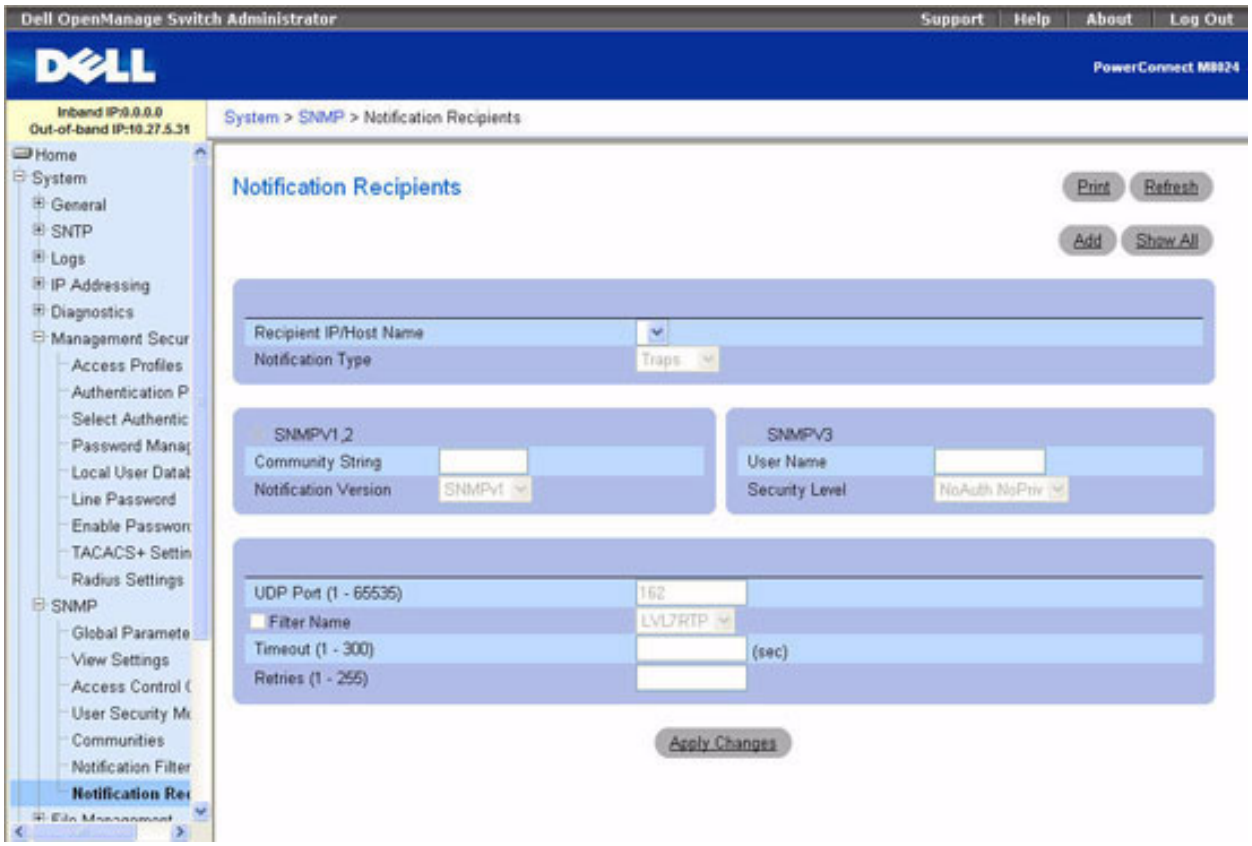
Use the **Notification Recipients** page to view information for defining filters that determine whether traps are sent to specific users, and the trap type sent. SNMP notification filters provide the following services:

- Identifying Management Trap Targets
- Trap Filtering
- Selecting Trap Generation Parameters
- Providing Access Control Checks

To display the **Notification Recipients** page, click **System > SNMP > Notification Recipient** in the tree view.

Downloaded from www.Manualslib.com manuals search engine

Figure 6-106. Notification Recipients



The **Notification Recipients** page contains the following fields:

- **Recipient IP —** Contains a user-defined list of notification recipients IP addresses.
- **Notification Type —** The type of notification sent. The possible field values are:
  - **Trap —** Traps are sent.
  - **Inform —** Informs are sent.
- **SNMPv1,2 —** SNMP versions 1 or 2 are enabled for the selected recipient. The possible field values are:
  - **Community String —** Displays the community string to be sent with the notification.
  - **Notification Version —** Determines the notification version. The possible field values are:
    - **SNMP V1 —** SNMP version 1 traps are sent. If Inform is selected as the Notification Type, SNMPv1 cannot be selected.
    - **SNMP V2 —** SNMP version 2 traps or informs are sent.
- **SNMPv3 —** SNMP version 3 is enabled for the selected recipient. The possible field values are:
  - **User Name —** Select the existing user to generate notifications.

Downloaded from www.Manualslib.com manuals search engine

– **Security Level** — The security level attached to notifications. The possible field values are:
  - **NoAu NoPriv** — The packet is neither authenticated nor encrypted.
  - **Auth NoPriv** — The packet is authenticated.
  - **Auth Priv** — The packet is both authenticated and encrypted.

- **UDP Port (1–65535)** — UDP port used to send notifications. The default is 162.
- **Filter Name** — Check this check box to apply a user-defined SNMP filter (selected from the drop-down menu) to notifications.
- **Timeout (1–300)** — Amount of time (seconds) the device waits before resending informs. The default is 15 seconds.
- **Retries (1–255)** — Maximum number of times the device resends an inform request. The default is 3.

Adding a New Notification Recipient

1. Open the **Notification Recipients** page.
2. Click **Add.**

   The **Notification Recipients** page displays:

Figure 6-107. Add Notification Recipient

3. Define the relevant fields.

Downloaded from www.Manualslib.com manuals search engine

4. Click **Apply Changes**.

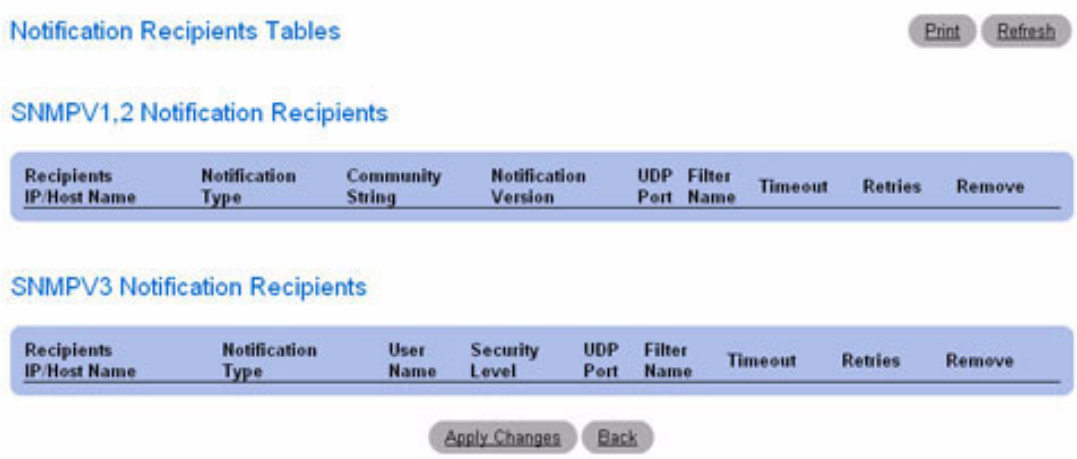
   The notification recipient is added, and the device is updated.

Displaying the Notification Recipients Tables

1. Open **Notification Recipients** page.
2. Click **Show All**.

   The **Notification Recipient Tables** page opens:

Figure 6-108. Notification Recipient Tables



Removing Notification Recipients

1. Open the **Notification Recipients** page.
2. Click **Show All**.

   The **Notification Recipient Tables** page open.
3. Select the **Remove** check box for one or more notification recipients in the **SNMPV1,2 Notification Recipient** and/or **SNMPv3 Notification Recipient Tables**.
4. Click **Apply Changes**.

   The recipients are removed, and the device is updated.

Defining SNMP Notification Recipients Using CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- SNMP Commands.

Downloaded from www.Manualslib.com manuals search engine

File Management

Use the **File Management** menu page to manage device software, the image file, and the configuration files. In addition to a TFTP server, the file management feature has been enhanced to allow file uploads and downloads by using an HTTP session (in other words, by using your web browser).

Configuration file transfers are also permitted by using Secure Copy (SCP) and SSH File Transfer Protocol (SFTP).

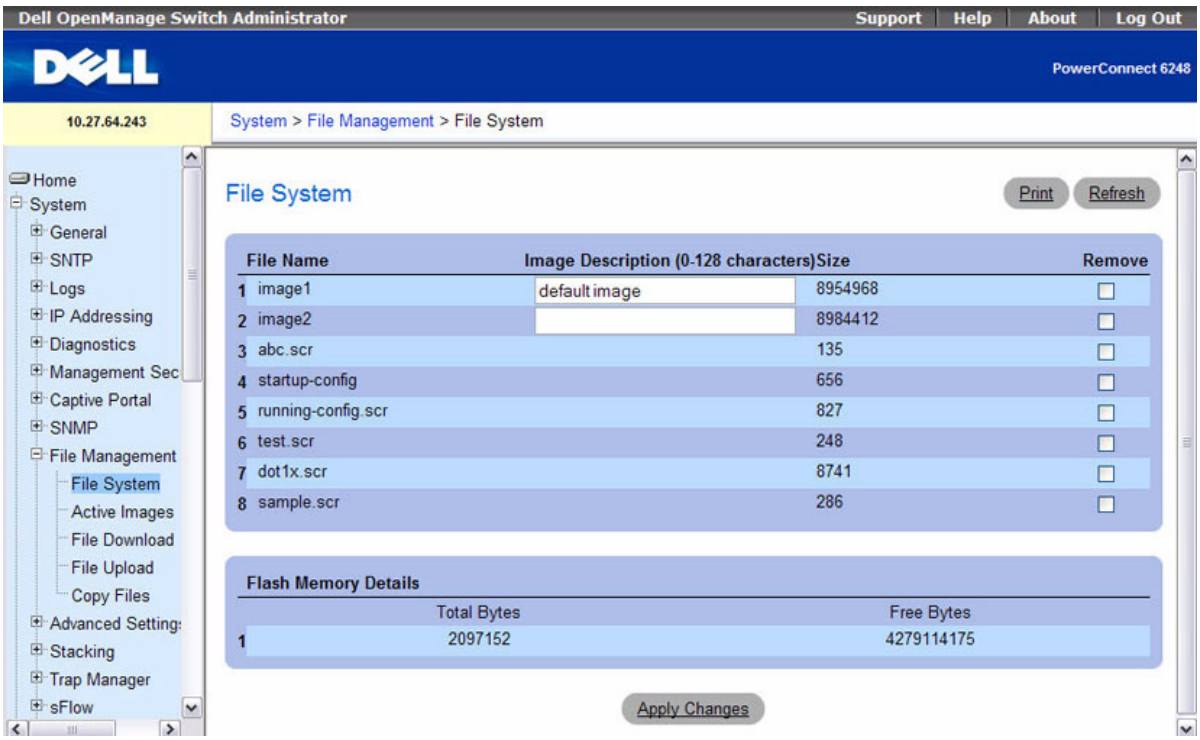
The system handles two versions of the software image. The system running an older software version will ignore (not load) a configuration file created by the newer software version. When a configuration file created by the newer software version is discovered by the system running an older version of the software, the system will display an appropriate warning to the user.

File System

Use the **File System** page to view a list of the files on the device.

To display the **File System** page, click **System** > **File Management** > **File System** in the tree view.

Figure 6-109. File System



The **File System** page contains the following fields:

- **File Name** — A text field listing the names of the files on the file system.

Downloaded from www.Manualslib.com manuals search engine

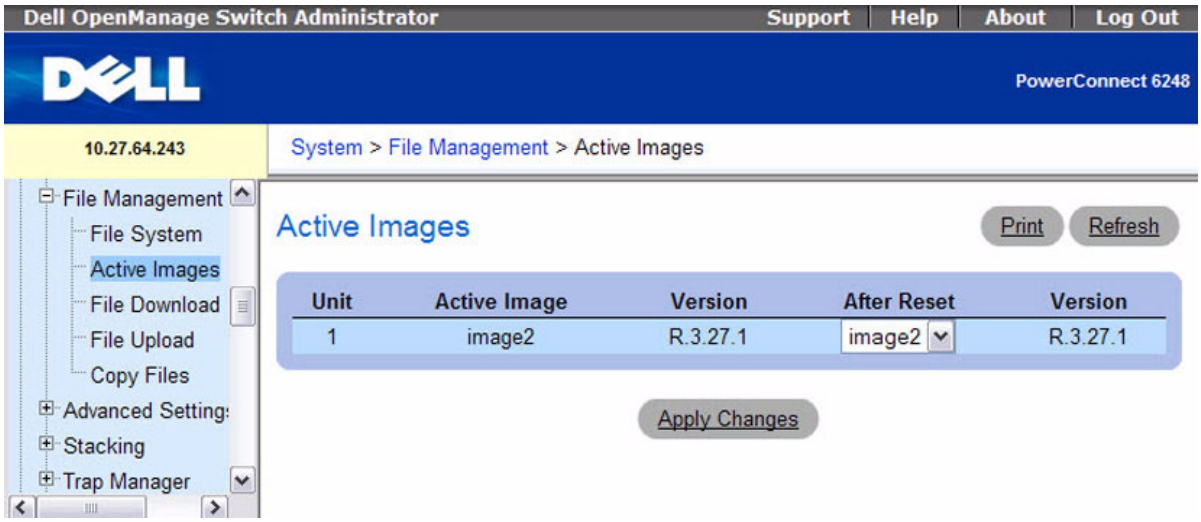
- **Image Description —** A field 0-128 characters in length that displays an image description of the file.
- **Size —** Displays the size of the specified file in bytes.
- **Remove —** Select to remove the specified file.
- **Flash Memory Details —** Displays Flash Memory availability details, in terms of total bytes of memory used, and memory (in bytes) available.

Active Images

Use the **Active Images** page to set the boot image.

To display the **File System** page, click **System** > **File Management** > **Active Images** in the tree view.

Figure 6-110. Active Images



The **Active Images** page contains the following fields:

- **Unit —** The unit on which the active image is running.
- **Active Image —** The name of the current active image.
- **Version —** The version of the current active image.
- **After Reset —** From the menu, select the image that should be active after the next reset.
- **Version —** Displays the version of the image after reset.

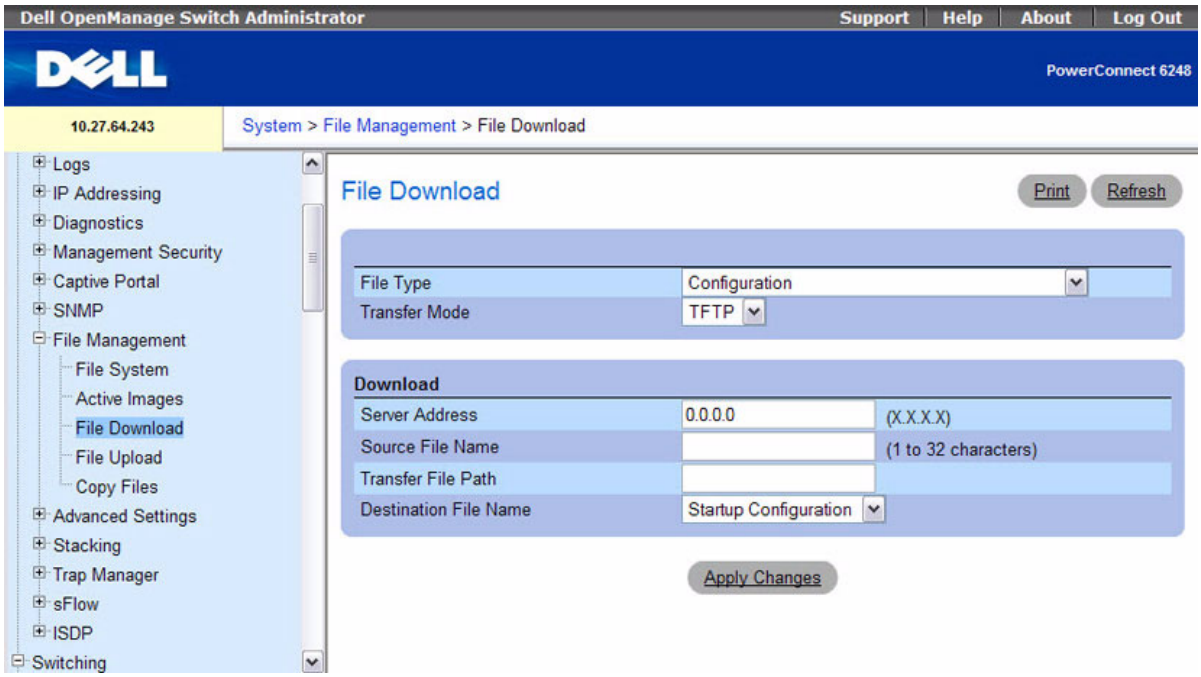
File Download

Use the **File Download** page to download image (binary) files, SSH and SSL certificates, and configuration (ASCII), files from the server to the device.

To display the **File Download** page, click **System** > **File Management** > **File Download** in the tree view.

Downloaded from www.Manualslib.com manuals search engine

Figure 6-111. File Download



The **File Download** page contains the following fields:

File Type — Select the type of file to be downloaded. Possible filetypes are:

- **Firmware** — Downloads the active image.
- **SSH-1 RSA Key File** — SSH-1 Rivest-Shamir-Adleman (RSA) Key File
- **SSH-2 RSA Key PEM File** — SSH-2 Rivest-Shamir-Adleman (RSA) Key File (PEM Encoded)
- **SSH-2 DSA Key PEM File** — SSH-2 Digital Signature Algorithm (DSA) Key File (PEM Encoded)

  NOTE: To download SSH key files, SSH must be administratively disabled and there can be no active SSH sessions.

- **SSL Trusted Root Certificate PEM File** — SSL Trusted Root Certificate File (PEM Encoded)
- **SSL Server Certificate PEM File** — SSL Server Certificate File (PEM Encoded)
- **SSL DH Weak Encryption Parameter PEM File** — SSL Diffie-Hellman Weak Encryption Parameter File (PEM Encoded)
- **SSL DH Strong Encryption Parameter PEM File** — SSL Diffie-Hellman Strong Encryption Parameter File (PEM Encoded)
- **Configuration** — Choose this option to update the switch's configuration. If the file has errors the update will be stopped. If **File Type - Configuration** and **Transfer Mode - HTTP** are selected, the **Destination File Name** field is also displayed.

Downloaded from www.Manualslib.com manuals search engine

- **Transfer Mode —** Select the file transfer mode for the configuration to download. The options are:
  - **TFTP** — Trivial File Transfer Protocol
  - **SFTP** — SSH File Transfer Protocol
  - **SCP** — Secure Copy
  - **HTTP** — Download files of various types to the switch using an HTTP session (in other words, by using your web browser).
- **Server Address** — Specify the TFTP/SFTP/SCP server IP address from which the configuration files are downloaded.
- **Source File Name —** Name of the file on the TFTP/SFTP/SCP server. The name can be from 1 to 32 characters.
- **Transfer File Path** — Specify the path of the file to be downloaded from the TFTP/SFTP/SCP server.
- **User Name** — Name of the user on the server. Used for authentication in case of SFTP/SCP server.
- **Password** — Password of the user on the server. Used for authentication in case of SFTP/SCP server.
- **Destination File Name** — The destination file to which to the configuration file is downloaded. Possible values are:
  - **Startup Configuration** — Downloads the startup configuration files.
  - **Backup Configuration** — Downloads the backup configuration files.
- **Select File** — Used in case of HTTP download. Enter the path and filename or browse for the file you want to download. You may enter up to 80 characters.

Click **Apply Changes** to initiate the file download.

NOTE: HTTP File Download is not available by using the CLI.

Downloading Files

1. Open the **File Download From Server** page.
2. Verify the IP address of the server and ensure that the software image or boot file to be downloaded is available on the server.
3. Complete the **Server Address** and **Source File Name** (full path without server IP address) fields.
4. If you are downloading a configuration file, select the **Destination File Name**.
5. Click **Apply Changes**.

   NOTE: After you start a file download, the page refreshes and a transfer status field appears to indicate the number of bytes transferred. The Web interface is blocked until the file download is complete.
6. The software is downloaded to the device.

Downloaded from www.Manualslib.com manuals search engine

Downloading Files Using CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

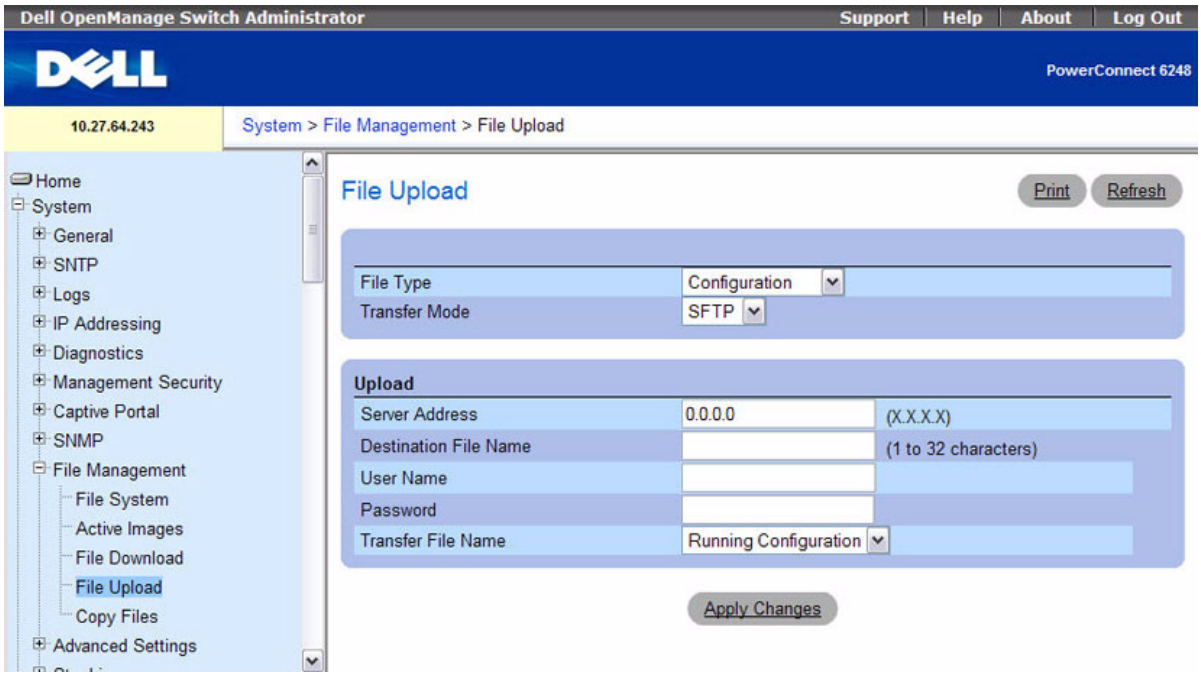
- Configuration and Image Files Commands.

File Upload

Use the **File Upload to Server** page to upload configuration (ASCII), image (binary), operational log, and startup log files from the device to the server.

To display the **File Upload to Server** page, click **System > File Management > File Upload** in the tree view.

Figure 6-112. File Upload to Server



The **File Upload to Server** page contains the following fields:

- **File Type —** Select the type of file to be uploaded. Possible filetypes are:
  - **Firmware** — Uploads the active image.
  - **Configuration** — Uploads the configuration file. If **File Type - Configuration** is selected, the **Transfer File Name** field is also displayed.
  - **Startup Log** — Uploads the startup log file.
  - **Operational Log** — Uploads the operational log.
- **Transfer Mode —** Select the transfer mode to upload the file to the server. The options are:

Downloaded from www.Manualslib.com manuals search engine

- **TFTP** — Trivial File Transfer Protocol
- **SFTP** — SSH File Transfer Protocol
- **SCP** — Secure Copy
- **HTTP**— Hypertext Transfer Protocol

Upload

Upload contains the following fields:

- **Server Address** — The server IP address to which the selected file is uploaded.
- **Destination File Name —** The name which the file will have after it is uploaded. The name can be **1 – 32 characters.**
- **User Name** — Name of the user on the server. Used for authentication in case of SFTP/SCP server.
- **Password** — Password of the user on the server. Used for authentication in case of SFTP/SCP server.
- **Transfer File Name —** Select the source configuration file to upload. Valid field values are:
  - **Running Configuration** — Uploads the running configuration file.
  - **Startup Configuration** — Uploads the startup configuration files.
  - **Backup Configuration** — Uploads the backup configuration files.

Uploading Files

1. Open the **File Upload to Server** page.
2. Define the applicable fields in the page.
3. Click **Apply Changes**.

NOTE: After you start a file upload, the page refreshes and a transfer status field appears to indicate the number of bytes transferred. The Web interface is blocked until the file upload is complete.

4. The software is uploaded to the server.

Uploading Files Using CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- Configuration and Image Files Commands.

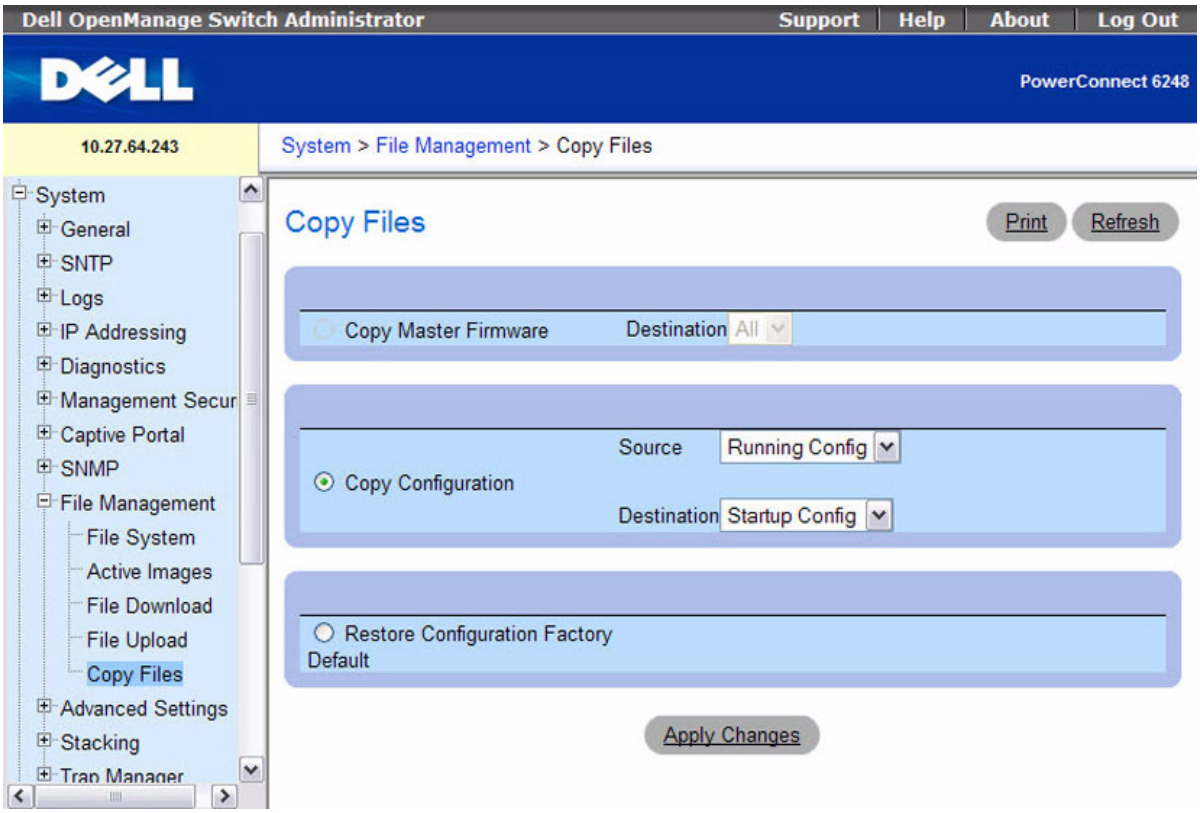
Copy Files

The Copy Files page not only provides a method for copying files within the file system, but also to and from remote servers. You can also backup images to local or remote systems or restore images from local or remote systems.

To display the **Copy Files** page, click **System > File Management > Copy Files** in the tree view.

Downloaded from www.Manualslib.com manuals search engine

Figure 6-113. Copy Files



The **Copy Files** page contains the following fields:

- **Copy Master Firmware** — Specifies that a software image file should be copied.
- **Destination** — The destination unit(s) (within the stack) to which the file is copied. Select from the menu one of the following values:
  - **All** — All units in the stack.
  - **Unit** — Specified unit within the stack, unit 1 for example.
- **Copy Configuration** — Specifies that a configuration file should be copied.
- **Source** — The configuration source file from which the file is copied. Select from the menu one of the following possible values:
  - **Running Config** — Uploads the running configuration file.
  - **Startup Config** — Uploads the startup configuration file.
  - **Backup Config** — Uploads the backup configuration file.
- **Destination** — The destination configuration file to which the file is copied. Select from the menu one of the following:

Downloaded from www.Manualslib.com manuals search engine

- **Startup Config —** The startup configuration file.
- **Backup Config —** The backup configuration file.

- **Restore Configuration Factory Default —** Select the radio button and click **Apply Changes** to restore all configuration structures to the defaults.

Defining Advanced Settings

Use Advanced Settings to set miscellaneous global attributes of the device. The changes to these attributes are applied only after the device is reset. Click **System > Advanced Settings** in the tree view to display the **Advanced Settings** page.

The **Advanced Settings** page contains a link for configuring Auto Configuration.

Auto Configuration

The Auto Configuration feature enables the configuration of a switch automatically when the device is turned on and, during the boot process, no configuration file is found in device storage. By communicating with a DHCP server, obtains an IP address for the switch and an IP address for a TFTP server. Auto Configuration attempts to download a configuration file from the TFTP server and install it on the switch.

The DHCP server that the switch communicates with must provide the following information:

- The IP address and subnet mask (option 1) to be assigned to the switch.
- The IP address of a default gateway (option 3), if needed for IP communication.
- The identification of the TFTP server from which to obtain the boot file. This is given by any of the following fields, in the priority shown (highest to lowest):
  - The sname field of the DHCP reply.
  - The hostname of the TFTP server (option 66). Either the TFTP address or name is specified—not both—in most network configurations. If a TFTP hostname is given, a DNS server is required to translate the name to an IP address.
  - The IP address of the TFTP server (option 150).
  - The address of the TFTP server supplied in the siaddr field.
  - The name of the configuration file (boot file or option 67) to be downloaded from the TFTP server. The boot file name must have a file type of *.cfg.
- The IP addresses of DNS name servers (option 6). The IP addresses of DNS name servers should be returned from the DHCP server only if the DNS server is in the same LAN as the switch performing Auto Configuration. A DNS server is needed to resolve the IP address of the TFTP server if only the “sname” or option 66 values are returned to the switch.

After obtaining IP addresses for both the switch and the TFTP server, the Auto Configuration feature attempts to download a host-specific configuration file using the boot file name specified by the DHCP server. If the switch fails to obtain the file, it will retry indefinitely.

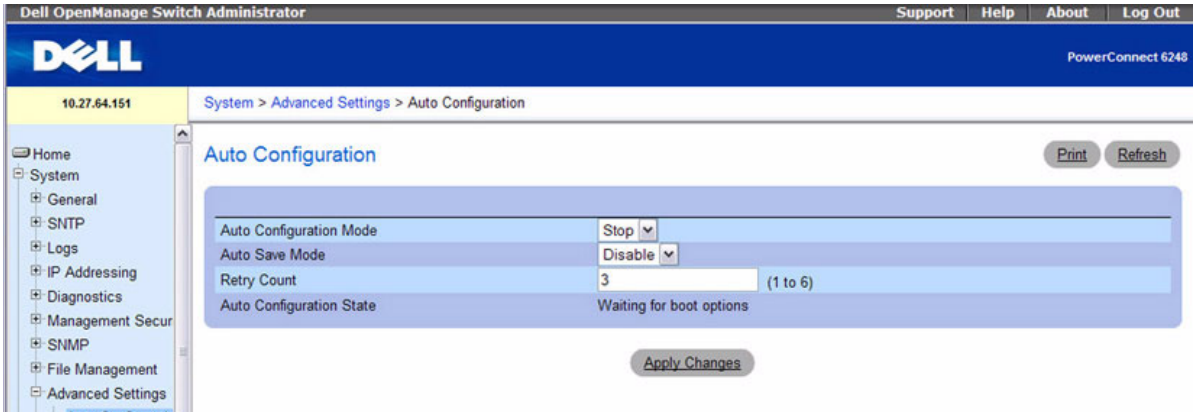
Downloaded from www.Manualslib.com manuals search engine

Use the **Auto Configuration** page to enable the switch to be automatically configured when it is initialized and cannot find a configuration file. With Auto Configuration enabled, the switch obtains an IP address and downloads a configuration file from a TFTP server.

NOTE: The Auto Configuration process requires the DHCP client on the switch to be enabled by default. The Auto Configuration feature also depends upon the configuration of other devices in the network, including a DHCP or BOOTP server, a TFTP server and, if necessary, a DNS server.

To display the **Auto Configuration** page, click **System** > **Advanced Settings** > **Auto Configuration** in the tree view.

Figure 6-114. Auto Configuration



The **Auto Configuration** page contains the following fields:

- **Auto Configuration Mode —** Enables (Start) or disables (Stop) the Auto Configuration feature on the switch. Select Start to initiate sending a request to a DHCP server to obtain an IP address of a server and the configuration file name. If it obtains the server address, Auto Configuration proceeds to search for and download a configuration file from the server. If successful, it applies the configuration file to the switch. After starting the Auto Configuration process, you can monitor the status of the process by the messages in the Auto Configuration State and Retry Count fields.
- **Auto Save Mode** — Specifies whether to save the automatically downloaded configuration file to the startup configuration.
  - **Enable** — Automatically saves the configuration file to the startup configuration.
  - **Disable** — Uses the configuration file as the running configuration only. When the switch reboots, it will load the configuration from the startup configuration file.
- **Retry Count** — Indicates the number of times to attempt the auto configuration process during boot up. The number of times the switch has attempted to contact the TFTP server during the current Auto Configuration session.
- **Auto Configuration State —** Shows the current state of the Auto Configuration process.

Downloaded from www.Manualslib.com manuals search engine

Configuring Auto Configuring Using the CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- Utility Commands

Defining Stacking

Use the Stacking menus to set the stacking characteristics of the device. The changes to these attributes are applied only after the device is reset. **System > Stacking** in the tree view to display the **Stacking** page. Use this page to go to the following features:

- Stacking Standby
- Unit Configuration
- Stack Summary
- Supported Switches
- Stack Port Summary
- Stack Port Counters
- Stack Port Diagnostics

NOTE: The PowerConnect M8024 does not support stacking.

Stacking Standby

You can now select a unit in the stack to be the Standby switch. The unit configured as the Standby switch becomes the stack manager if the current manager fails. To remove the selected unit as the Standby switch, click Delete.

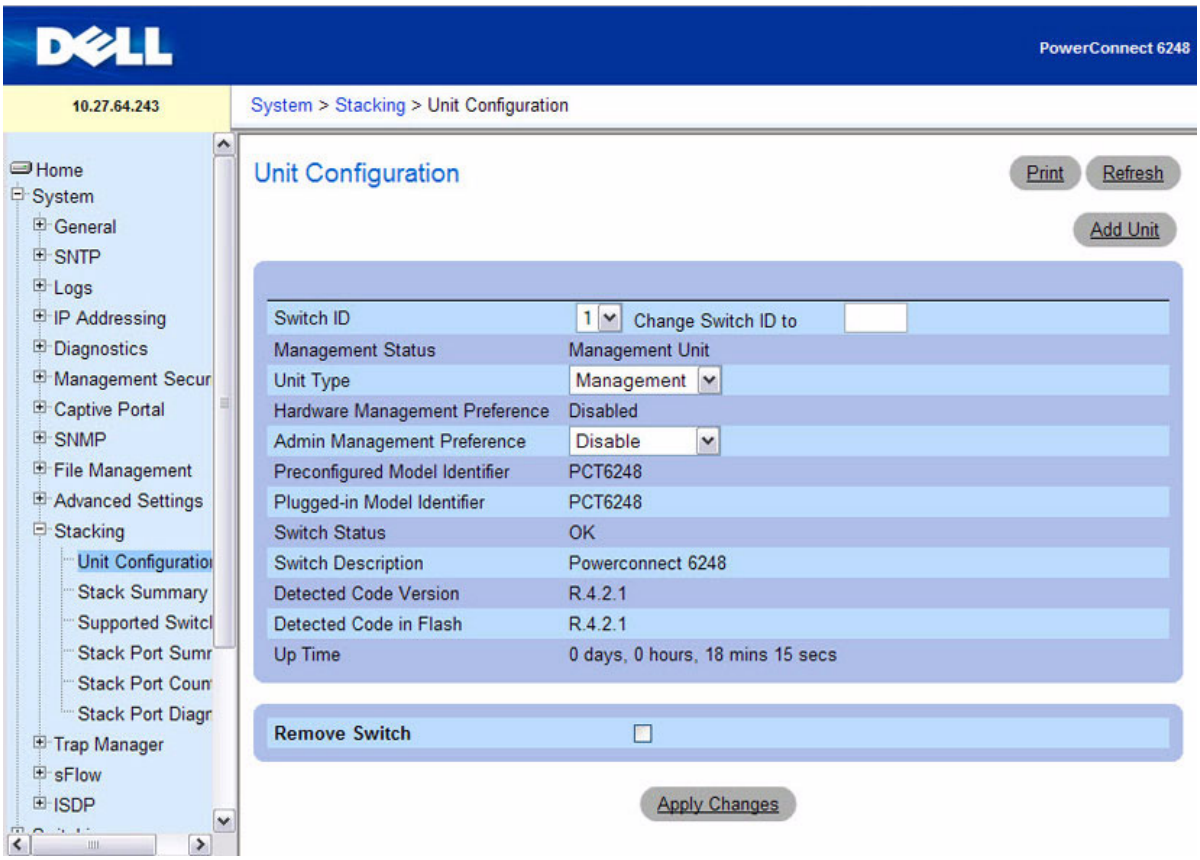
Unit Configuration

Use the **Unit Configuration** page to define general device parameters.

To display the **Unit Configuration** page, click **System > Stacking > Unit Configuration** in the tree view.

Downloaded from www.Manualslib.com manuals search engine

Figure 6-115. Unit Configuration



The **Unit Configuration** page contains the following fields:

- **Switch ID —** Specifies unit to be configured.
- **Change Switch ID to —** Changes the unit number of the selected unit.
- **Management Status —** Shows whether the selected unit is a Management Unit or a Stack Member.
- **Unit Type** — Specify whether the select unit is the Management Unit (Stack Master), a Stack Member, or the Standby Switch.
- **Hardware Management Preference —** Management preference by hardware configuration to be considered for selection as Management unit.
- **Admin Management Preference —** Determines whether this unit is capable of becoming the master switch. Values range from **Disable** (the unit cannot support Master Switch function) to **Preference 15**. The higher value means that the unit is more desirable than another unit with lower value for running the management function. An additional value is **Unassigned**, which means that preference is not configured, and election of the Master is left to the stack units.
- **Preconfigured Model Identifier —** A 16-byte character string to identify the pre-configured model of the selected unit.

Downloaded from www.Manualslib.com manuals search engine

- **Plugged-in Model Identifier** — A 16-byte character string to identify the plugged-in model of the selected unit.
- **Switch Status** — Displays the status of the selected unit. The possible values are:
  - **OK** — The unit is in place and functioning.
  - **Unsupported** — The unit is in place, but can not function as a member of the stack.
  - **Code Mismatch** — The software of the switch does not match the master unit software.
  - **Config Mismatch** — The configuration of the switch does not match the master unit configuration.
  - **Not Present** — The selected unit is not present.
- **Switch Description** — 80-byte data field used to identify the device.

Expected Code Type — Displays the expected code identifier.

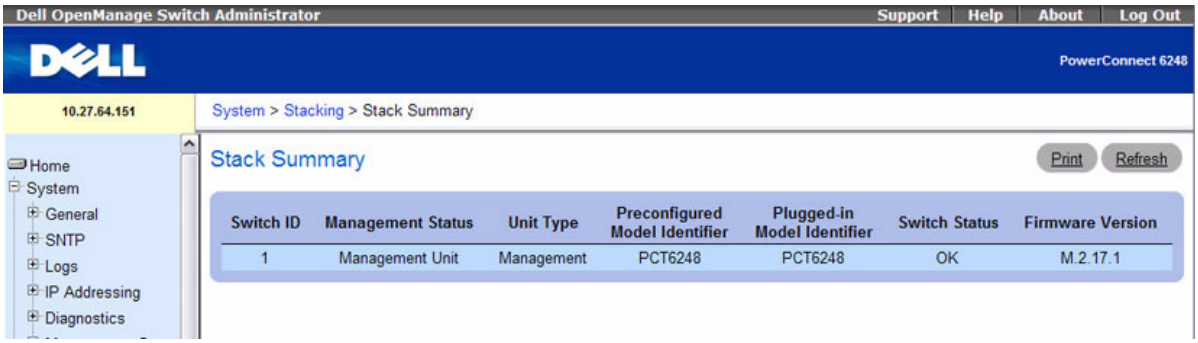
- **Detected Code Version** — Running code version release number and version number.
- **Detected Code in Flash** — Release number and version number of the code detected in flash.
- **Up Time** — Displays how long the unit has been running since its last reset.
- **Remove Switch** — Select this option to remove switch from the stack.

Stack Summary

Use the **Stack Summary** page to view a summary of switches participating in the stack.

To display the **Stack Summary** page, click **System** > **Stacking** > **Stack Summary** in the tree view.

Figure 6-116. Stack Summary



The **Stacking Summary** page contains the following fields:

- **Switch ID** — ID of the unit. The maximum number of units allowed in the stack is 8.
- **Management Status** — This field indicates whether the switch is currently operating as the management switch, the standby switch, or a stack member.
- **Standby Status** — This field identifies the switch that is configured as the Standby Unit. Possible values are:

Downloaded from www.Manualslib.com manuals search engine

- OPR Standby — Indicates that this unit is operating as the Standby Unit and the configured Standby Unit is not part of the stack.
- CFG Standby — Indicates that the unit is configured as the Standby Unit. The unit configured as the Standby switch becomes the stack manager if the current manager fails.
- Blank — Indicates that the switch is not configured as the Standby Unit.

- **Unit Type**— This field indicates whether the switch is configured as the management switch, the standby switch, or a stack member.
- **Pre-configured Model Identifier** — This field displays the 16-character field assigned by the device manufacturer to identify the pre-configured device.
- **Plugged-in Model Identifier** — This field displays the 16-character field assigned by the device manufacturer to identify the plugged-in device.
- **Switch Status** — Indicates the unit status. There are five possible state values:
  - OK — The unit is in place and functioning properly.
  - Unsupported — The unit is not allowed to stack.
  - Code Mismatch — The software image in this unit does not match that being used in the master switch of the stack.
  - Config Mismatch — The configuration file in this unit do not match that being used in the master switch of the stack.
  - Not Present — The unit is not there.
- **Firmware Version** — Indicates the detected version of code on this unit.

Viewing Stack Summary Using the CLI Command

For information about the CLI commands that perform this function, see the following chapter in the CLI Reference Guide:

- System Management Commands

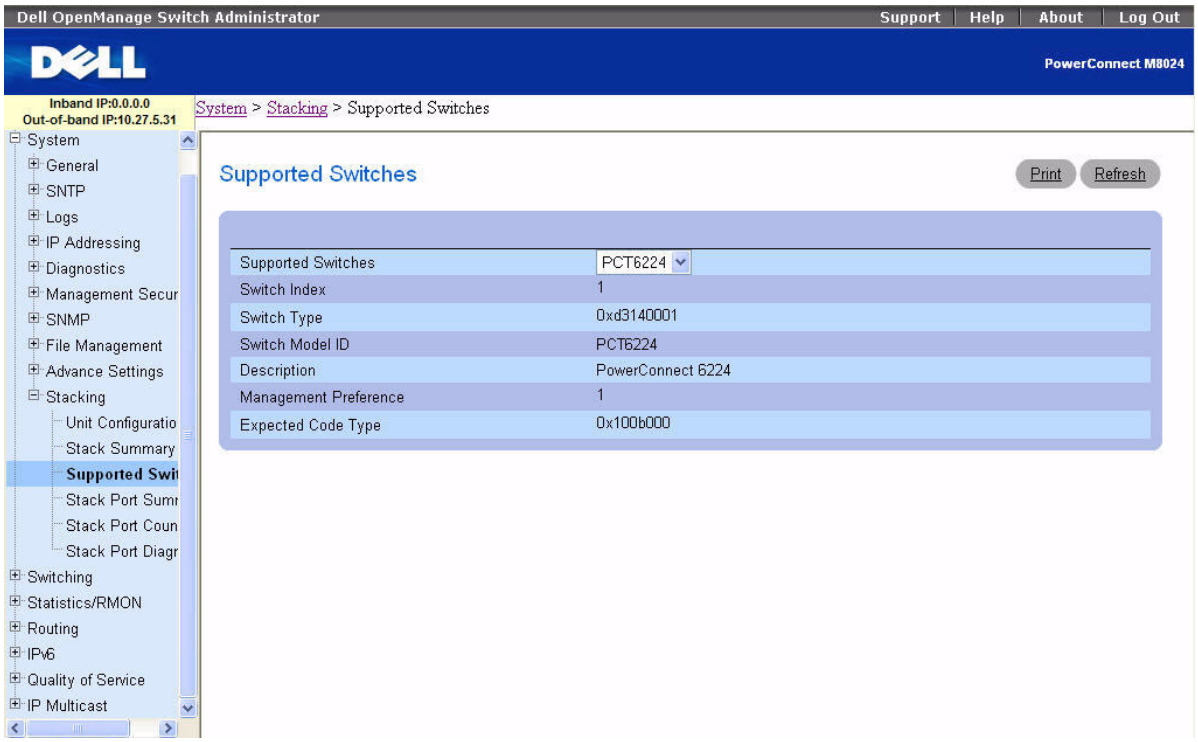
Supported Switches

Use the **Supported Switches** page to view information regarding each type of supported switch for stacking, and information regarding the supported switches.

To display the **Supported Switches** page, click **System** > **Stacking** > **Supported Switches** in the tree view.

Downloaded from www.Manualslib.com manuals search engine

Figure 6-117. Supported Switches



The **Supported Switches** page contains the following fields:

- **Supported Switches** — Drop-down list permits selection of switches supported.
- **Switch Index** — Specifies the index into the database of the supported switch types.
- **Switch Type** — Hardware ID given to the switch.
- **Switch Model ID** — Displays a 16-byte character string to identify the model of the supported switch.
- **Description** — Displays a 256-byte data field used to identify the device.
- **Management Preference** — Determines whether this unit is capable of becoming the master switch. If the value is set to zero then the unit cannot support Master Switch function. The higher value means that the unit is more desirable than another unit with lower value for running the management function. The device manufacturer sets the initial value of this field.
- **Expected Code Type** — Displays the release number and version number of the code expected.

Viewing Supported Switch Characteristics

1. Open the **Supported Switches** page.
2. Select desired switch from the **Supported Switch** drop-down list.

Downloaded from www.Manualslib.com manuals search engine

Viewing Supported Switches Using the CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the CLI Reference Guide:

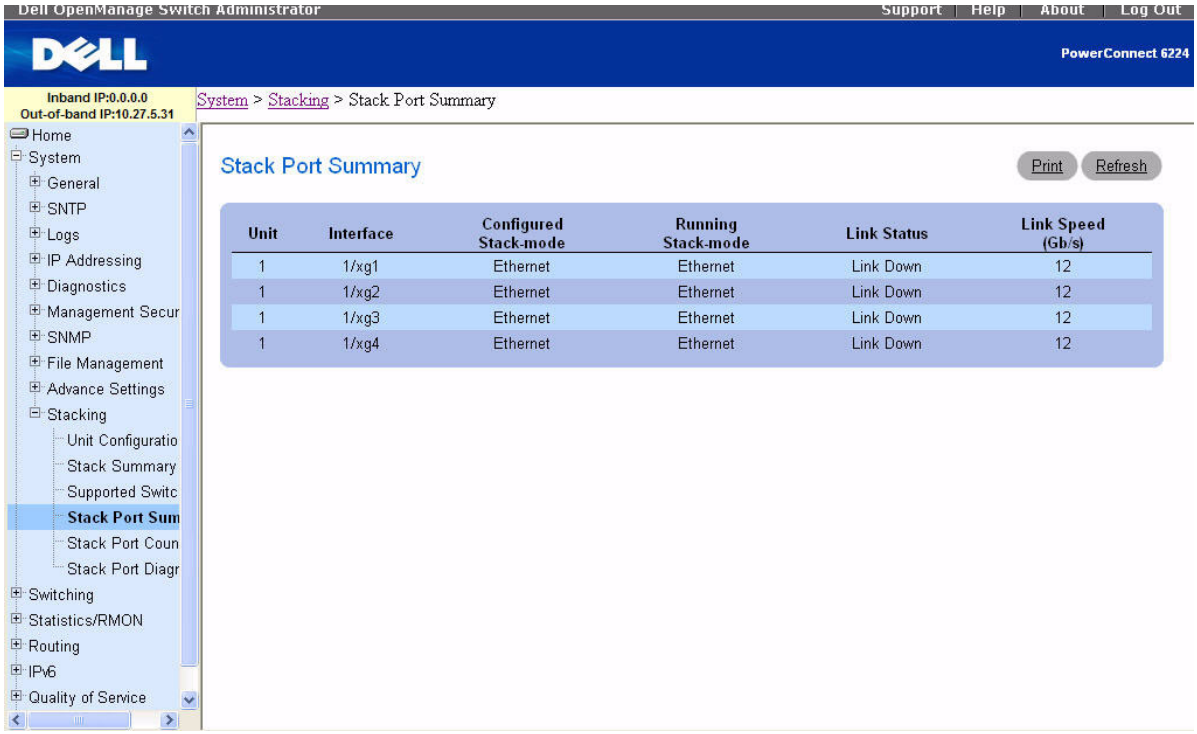
- System Management Commands

Stack Port Summary

Use the **Stack Port Summary** page to view the stackable ports present. This screen displays the unit, the stackable interface, the configured mode of the interface, the running mode as well as the link status and link speed of the stackable port.

To display the **Stack Port Summary** page, click **System > Stacking > Stack Port Summary** in the tree view.

Figure 6-118. Stack Port Summary



The **Stack Port Summary** page contains the following fields:

- **Unit** — ID number of the unit.
- **Interface —** Identifies the stack interface assigned to the unit.
- **Configured Stack Mode (configurable only on the PowerConnect M6348)** — Indicates whether or not each unit is able to participate in the stack.
- **Running Stack Mode** — Indicates whether or not each unit is actually participating in the stack.

Downloaded from www.Manualslib.com manuals search engine

- **Link Status** — Indicates whether or not the stack interface for each unit is operating.
- **Link Speed (Gb/s)** — Indicates the nominal speed of each unit's link.

Viewing Stack Port Summary Using the CLI Command

For information about the CLI commands that perform this function, see the following chapter in the CLI Reference Guide:

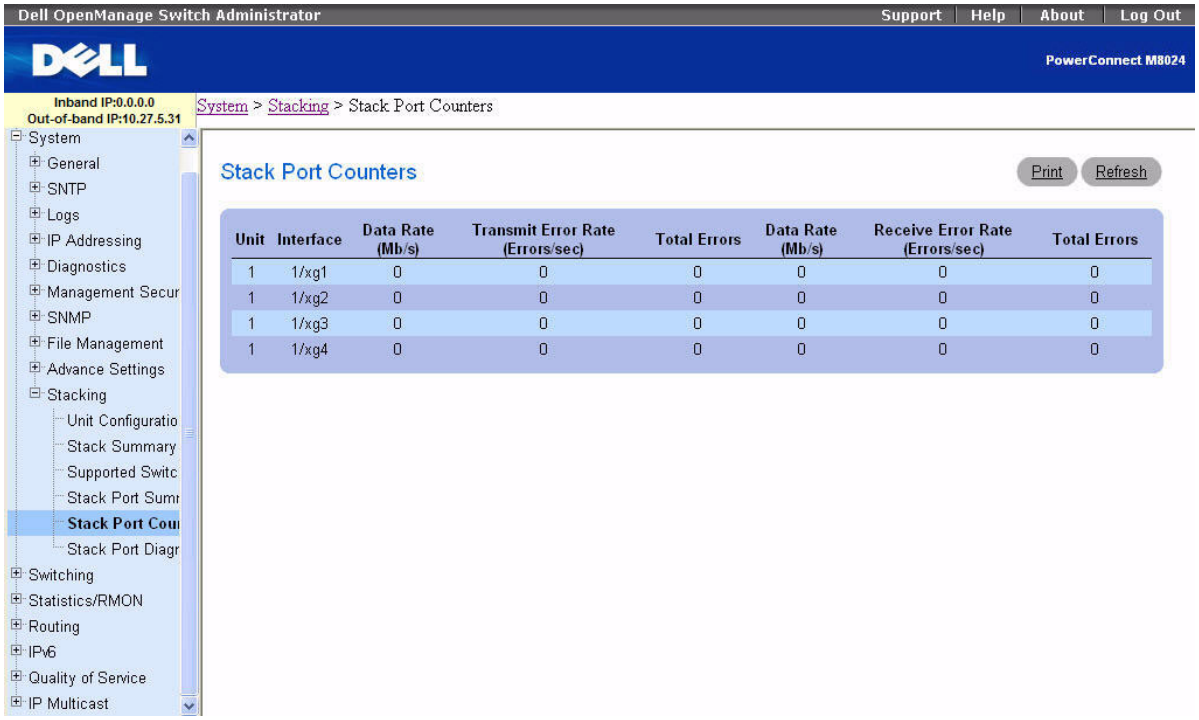
- System Management Commands

Stack Port Counters

Use the **Stack Port Counters** page to view the transmitted and received statistics, including data rate and error rate.

To display the **Stack Port Counters** page, click **System > Stacking > Stack Point Counters** in the tree view.

Figure 6-119. Stack Port Counters



Unit	Interface	Data Rate (Mb/s)	Transmit Error Rate (Errors/sec)	Total Errors	Data Rate (Mb/s)	Receive Error Rate (Errors/sec)	Total Errors
1	1/xg1	0	0	0	0	0	0
1	1/xg2	0	0	0	0	0	0
1	1/xg3	0	0	0	0	0	0
1	1/xg4	0	0	0	0	0	0

The **Stack Port Counters** page contains the following fields:

- **Unit** — Indicates the subordinate switch being viewed.
- **Interface** — Indicates the name of the interface.
- **Data Rate (Mb/s)** — Indicates the speed at which the data is transmitted.

Downloaded from www.Manualslib.com manuals search engine

- **Transmit Error Rate (Errors/sec)** — Indicates the number of errors transmitted per second.
- **Total Errors** — Total number of errors transmitted.
- **Data Rate (Mb/s)** — Indicates the speed at which the data is received.
- **Receive Error Rate (Errors/sec)** — Indicates the number of errors received per second.
- **Total Errors** — Total number of errors received.

Viewing Stack Port Counters

1. Open the **Stack Port Counters** page.

Viewing Stack Port Counters Using the CLI Command

For information about the CLI commands that perform this function, see the following chapter in the CLI Reference Guide:

- System Management Commands

Stack Port Diagnostics

The **Stack Port Diagnostics** page is intended for Field Application Engineers (FAEs) and developers only.

sFlow

sFlow® is the standard for monitoring high-speed switched and routed networks. sFlow technology is built into network equipment and gives complete visibility into network activity, enabling effective management and control of network resources.

The sFlow monitoring system consists of an sFlow Agent (embedded in a switch or router or in a standalone probe) and a central sFlow Collector. The sFlow Agent uses sampling technology to capture traffic statistics from the device it is monitoring. sFlow datagrams are used to immediately forward the sampled traffic statistics to an sFlow Collector for analysis.

The sFlow Agent uses two forms of sampling: statistical packet-based sampling of switched or routed Packet Flows, and time-based sampling of counters.

Advantages of using sFlow include the following:

- It is possible to monitor all ports of the switch continuously with no impact on the distributed switching performance.
- Very little memory/CPU is required. Samples are not aggregated into a flow-table on the switch; they are forwarded immediately over the network to the sFlow collector.
- The system is tolerant to packet loss in the network (statistical model means loss is equivalent to slight change in sampling rate).
- The sFlow collector can receive data from multiple switches, providing a real-time synchronized view of the whole network.

Downloaded from www.Manualslib.com manuals search engine

- The collector can analyze traffic patterns for whatever protocols are found in the headers (e.g. TCP/IP, IPX, Ethernet, AppleTalk…), which means there is no need for a layer 2 switch to decode and understand all protocols.

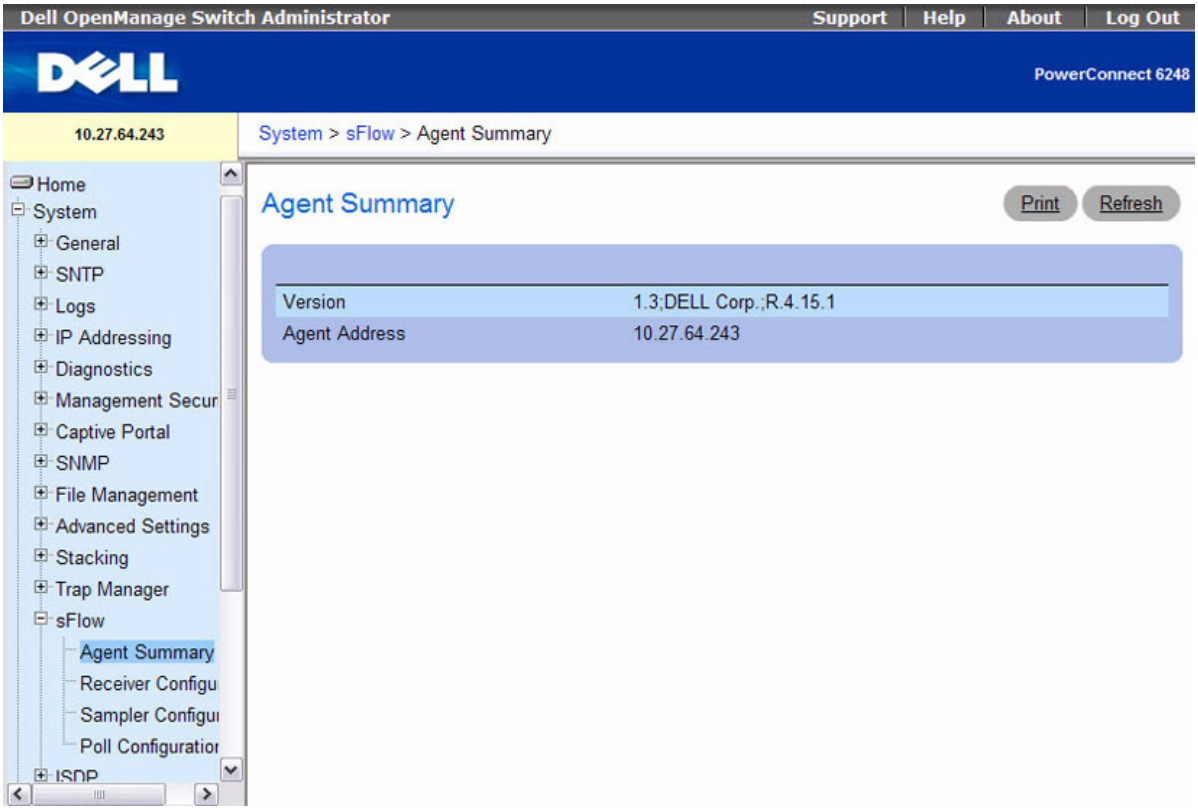
sFlow Agent Summary

Packet Flow Sampling and Counter Sampling are performed by sFlow Instances associated with individual data sources within the sFlow Agent. Packet Flow Sampling and Counter Sampling are designed as part of an integrated system. Both types of samples are combined in sFlow datagrams. Packet Flow Sampling will cause a steady, but random, stream of sFlow datagrams to be sent to the sFlow Collector. Counter samples may be taken opportunistically in order to fill these datagrams.

In order to perform Packet Flow Sampling, an sFlow Sampler Instance is configured with a Sampling Rate. The Packet Flow sampling process results in the generation of Packet Flow Records. In order to perform Counter Sampling, the sFlow Poller Instance is configured with a Polling Interval, The Counter Sampling process results in the generation of Counter Records. The sFlow Agent collects Counter Records and Packet Flow Records and sends them in the form of sFlow datagrams to sFlow Collectors.

To access the sFlow Agent Summary page, click **System > sFlow > Agent Summary** in the navigation tree.

Figure 6-120. sFlow Agent Summary



Downloaded from www.Manualslib.com manuals search engine

The **sFlow Agent Summary** page contains the following fields:

- **Version** — Uniquely identifies the version and implementation of this MIB. The version string must have the following structure: MIB Version; Organization; Software Revision where:
  - MIB Version — 1.3, the version of this MIB.
  - Organization — Dell Corp.
  - Revision — 1.0
- Agent Address — The IP address associated with this agent.

Configuring and Viewing sFlow Settings Using CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

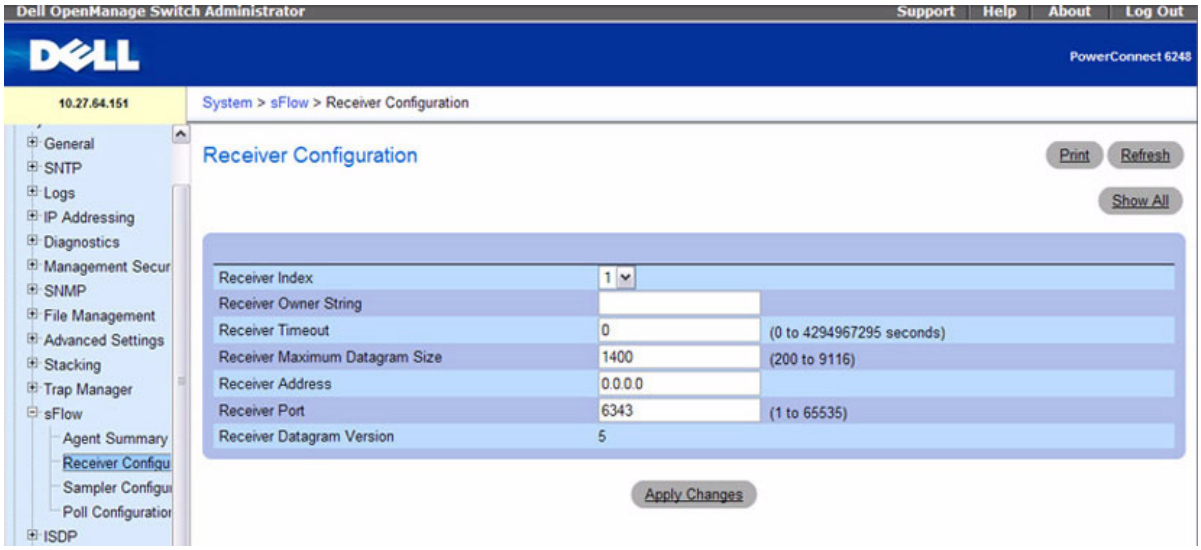
- sFlow Commands.

sFlow Receiver Configuration

Use the **sFlow Receiver Configuration** page to configure the sFlow Receiver.

To access the **sFlow Receiver Configuration** page, click **System > sFlow > Receiver Configuration** in the navigation tree.

Figure 6-121. sFlow Receiver Configuration



Downloaded from www.Manualslib.com manuals search engine

The **sFlow Receiver Configuration** page contains the following fields:

- **Receiver Index** — Selects the receiver for which data is to be displayed or configured. The allowed range is 1 to 8.
- **Receiver Owner String** — The entity making use of this sFlowRcvrTable entry. The empty string indicates that the entry is currently unclaimed and the receiver configuration is reset to the default values. An entity wishing to claim an sFlowRcvrTable entry must ensure that the entry is unclaimed before trying to claim it. The entry is claimed by setting the owner string. The entry must be claimed before any changes can be made to other sampler objects.
- **Receiver Timeout** — The time (in seconds) remaining before the sampler is released and stops sampling. A management entity wanting to maintain control of the sampler is responsible for setting a new value before the old one expires. The allowed range is 0 to 4294967295 seconds. A value of zero sets the selected receiver configuration to its default values.
- **Receiver Maximum Datagram Size** — The maximum number of data bytes that can be sent in a single sample datagram. The manager should set this value to avoid fragmentation of the sFlow datagrams. The default value is 1400. The allowed range is 200 to 9116.)
- **Receiver Address** — The IP address of the sFlow collector. If set to 0.0.0.0 no sFlow datagrams will be sent.
- **Receiver Port** — The destination port for sFlow datagrams. The allowed range is 1 to 65535).
- **Receiver Datagram Version** — The version of sFlow datagrams that should be sent.

Displaying the sFlow Receiver Summary Table

1. Open the **sFlow Receiver Configuration** page.
2. Click **Show All**.

   The **sFlow Receiver Summary** page displays:

Figure 6-122. sFlow Receiver Summary

sFlow Receiver Summary

Print Refresh

Receiver Index	Receiver Owner	Timeout	Maximum Datagram Size	Address	Port	Datagram Version
1		0	1400	0.0.0.0	6343	5
2		0	1400	0.0.0.0	6343	5
3		0	1400	0.0.0.0	6343	5
4		0	1400	0.0.0.0	6343	5
5		0	1400	0.0.0.0	6343	5
6		0	1400	0.0.0.0	6343	5
7		0	1400	0.0.0.0	6343	5
8		0	1400	0.0.0.0	6343	5

Back

Downloaded from www.Manualslib.com manuals search engine

Configuring and Viewing sFlow Settings Using CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- sFlow Commands.

sFlow Sampler Configuration

The sFlow Agent collects a statistical packet-based sampling of the switched flows and sends them to the configured receivers. A data source configured to collect flow samples is called a sampler.

Packet Flow Sampling

The Packet Flow Sampling mechanism carried out by each sFlow instance ensures that any packet observed at a Data Source has an equal chance of being sampled, irrespective of the Packet Flow(s) to which it belongs.

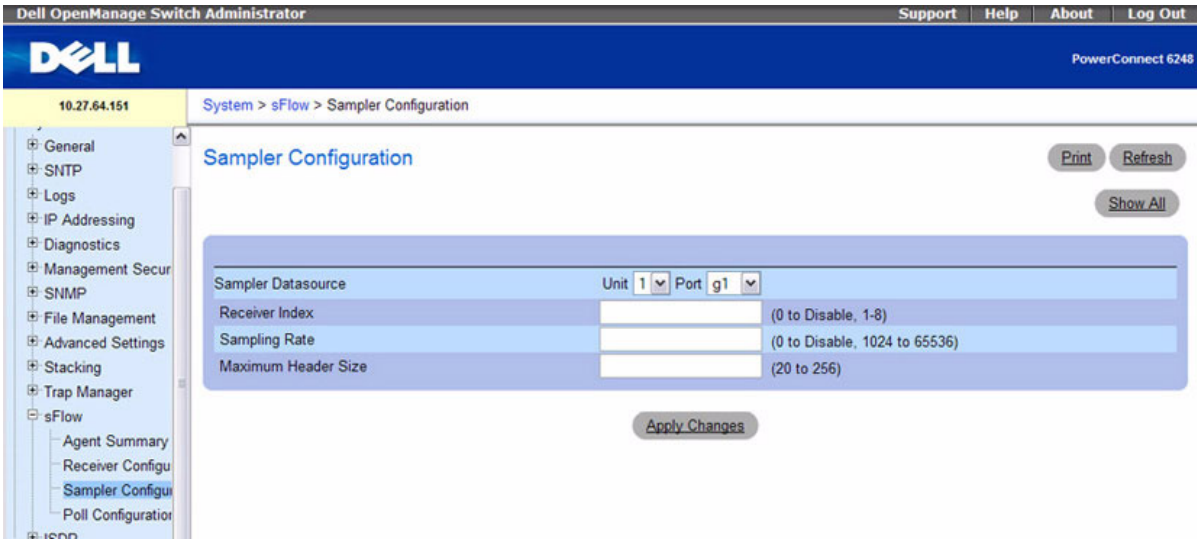
Packet Flow Sampling is accomplished as follows:

- When a packet arrives on an interface, the Network Device makes a filtering decision to determine whether the packet should be dropped.
- If the packet is not filtered (dropped), a destination interface is assigned by the switching/routing function.
- At this point, a decision is made on whether or not to sample the packet. The mechanism involves a counter that is decremented with each packet. When the counter reaches zero, a sample is taken. When a sample is taken, the counter that indicates how many packets to skip before taking the next sample is reset. The value of the counter is set to a random integer where the sequence of random integers used over time is the Sampling Rate.

To access the **sFlow Sampler Configuration** page, click **System > sFlow > Sampler Configuration** in the navigation tree.

Downloaded from www.Manualslib.com manuals search engine

Figure 6-123. sFlow Sampler Configuration



The **sFlow Sampler Configuration** page contains the following fields:

- **Sampler DataSource**— The sFlow data source for this sFlow sampler. This Agent supports physical ports only.
- **Receiver Index** — The sFlow Receiver for this sFlow sampler. If set to zero, no packets will be sampled. Only active receivers can be set. If a receiver expires, then all samplers associated with the receiver will also expire. The allowed range is 1 to 8.
- **Sampling Rate** — The statistical sampling rate for packet sampling from this source. A sampling rate of zero (0) disables sampling. The allowed range is 1024 to 65536.
- **Maximum Header Size** — The maximum number of bytes that should be copied from a sampled packet. The allowed range is 20 to 256.

Displaying the sFlow Sampler Summary Table

1. Open the **sFlow Sampler Configuration** page.
2. Click **Show All**.

   The **sFlow Sampler Summary** page displays:

Downloaded from www.Manualslib.com manuals search engine

Figure 6-124. sFlow Sampler Summary

sFlow Sampler Summary

Print Refresh

Sampler Datasource	Receiver Index	Sampling Rate	Maximum Header Size
1/g1	0	0	128
1/g2	0	0	128
1/g3	0	0	128
1/g4	0	0	128
1/g5	0	0	128
1/g6	0	0	128
1/g7	0	0	128
1/g8	0	0	128
1/g9	0	0	128
1/g10	0	0	128
1/g11	0	0	128

Configuring and Viewing sFlow Settings Using CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- sFlow Commands.

sFlow Poll Configuration

The sFlow agent collects time-based sampling of network interface statistics and sends them to the configured sFlow receivers. A data source configured to collect counter samples is called a poller.

Counter Sampling

The primary objective of Counter Sampling is to efficiently, periodically export counters associated with Data Sources. A maximum Sampling Interval is assigned to each sFlow instance associated with a Data Source.

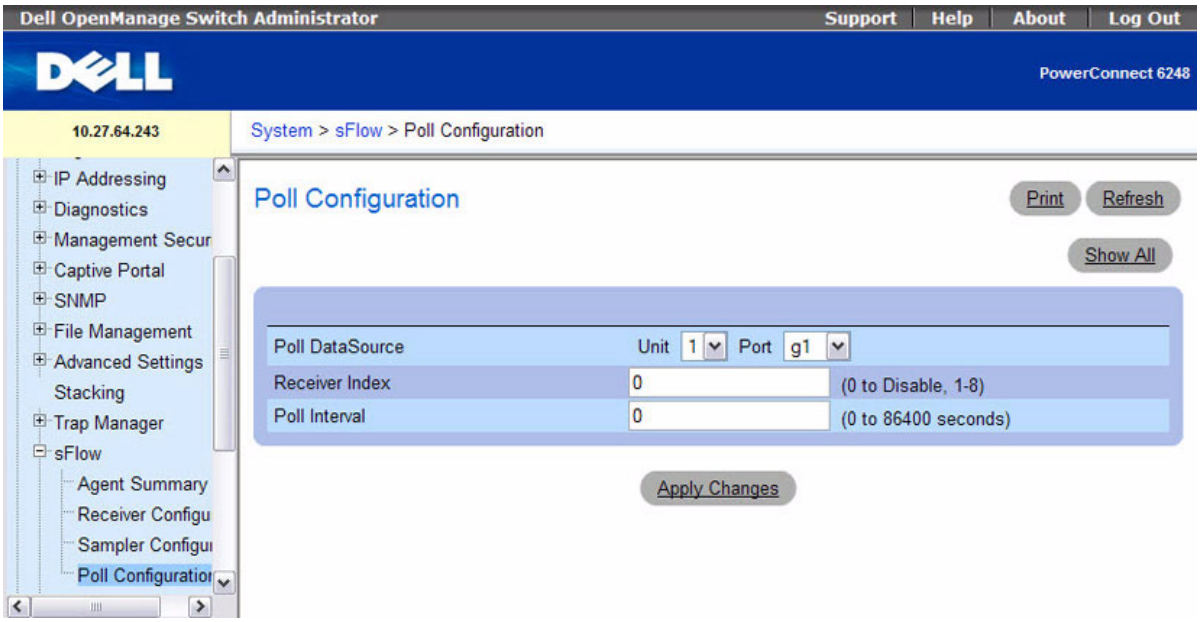
Counter Sampling is accomplished as follows:

The sFlow Agent keeps a list of counter sources being sampled. When a Packet Flow Sample is generated, the sFlow Agent examines the list and adds counters to the sample datagram, least recently sampled first. Counters are only added to the datagram if the sources are within a short period, i.e. five seconds, of failing to meet the required Sampling Interval. Periodically, i.e. every second, the sFlow Agent examines the list of counter sources and sends any counters that need to be sent to meet the sampling interval requirement.

To access the **sFlow Poll Configuration** page, click **System > sFlow > Poll Configuration** in the navigation tree.

Downloaded from www.Manualslib.com manuals search engine

Figure 6-125. sFlow Poll Configuration



The **sFlow Poll Configuration** page contains the following fields:

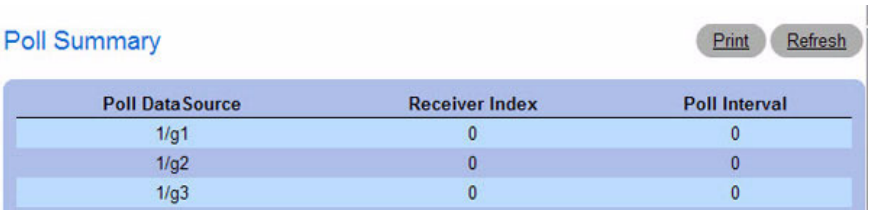
- **Poll DataSource**— The sFlow Sampler data source for this flow sampler. This Agent supports physical ports only.
- **Receiver Index** — The sFlowReceiver for this sFlow Counter Poller. If set to zero, the poller configuration is set to the default and the poller is deleted. Only active receivers can be set. If a receiver expires, then all pollers associated with the receiver will also expire. The allowed range is 1 to 8.
- **Poll Interval** — The maximum number of seconds between successive samples of the counters associated with this data source. The range is 0 to 86400 seconds.

Displaying the sFlow Poller Summary Table

1. Open the **sFlow Poll Configuration** page.
2. Click **Show All**.

   The **sFlow Poll Summary** page displays:

Figure 6-126. sFlow Poll Summary



Poll DataSource	Receiver Index	Poll Interval
1/g1	0	0
1/g2	0	0
1/g3	0	0

Downloaded from www.Manualslib.com manuals search engine

Configuring and Viewing sFlow Settings Using CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- sFlow Commands.

Industry Standard Discovery Protocol

The Industry Standard Discovery Protocol (ISDP) is a proprietary Layer 2 network protocol that inter-operates with Cisco® devices running the Cisco Discovery Protocol (CDP). ISDP is used to share information between neighboring devices. The switch software participates in the CDP protocol and is able to both discover and be discovered by other CDP-supporting devices.

The ISDP menu contains links to the following pages:

- ISDP Global Configuration
- Cache Table
- Interface Configuration
- ISDP Statistics

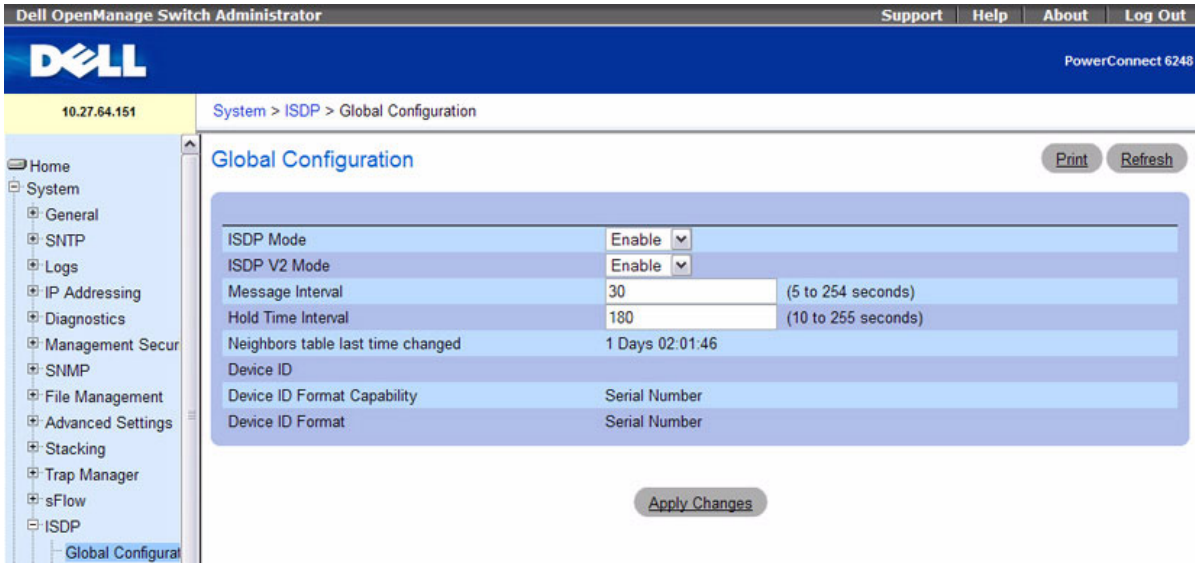
ISDP Global Configuration

From the **ISDP Global Configuration** page, you can configure the ISDP settings for the switch, such as the administrative mode.

To access the **ISDP Global Configuration** page, click **System > ISDP > Global Configuration** in the navigation tree.

Downloaded from www.Manualslib.com manuals search engine

Figure 6-127. ISDP Global Configuration



The **ISDP Global Configuration** page contain the following fields:

- **ISDP Mode** — Use this field to enable or disable the Industry Standard Discovery Protocol on the switch.
- **ISDP V2 Mode** — Use this field to enable or disable the Industry Standard Discovery Protocol v2 on the switch.
- **Message Interval** — Specifies the ISDP transmit interval. The range is (5–254). Default value is 30 seconds.
- **Hold Time Interval** — The receiving device holds ISDP message during this time period. The range is (10–255). Default value is 180 seconds.
- **Neighbors Table Last Time Changed** — Indicates when the Neighbors table entry was last modified.
- **Device ID** — The Device ID advertised by this device. The format of this Device ID is characterized by the value of Device ID Format object.
- **Device ID Format Capability** — Indicates the Device ID format capability of the device.
  - **serialNumber**—Indicates that the device uses serial number as the format for its Device ID.
  - **macAddress**—Indicates that the device uses layer 2 MAC address as the format for its Device ID.
  - **other**—Indicates that the device uses its platform specific format as the format for its Device ID.
- **Device ID Format** — Indicates the Device ID format of the device.
  - **serialNumber**—Indicates that the value is in the form of an ASCII string containing the device serial number.
  - **macAddress**—Indicates that the value is in the form of Layer 2 MAC address.

Downloaded from www.Manualslib.com manuals search engine

– **other**—Indicates that the value is in the form of a platform specific ASCII string containing info that identifies the device. For example: ASCII string contains serialNumber appended/prepended with system name.

Configuring ISDP Using CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

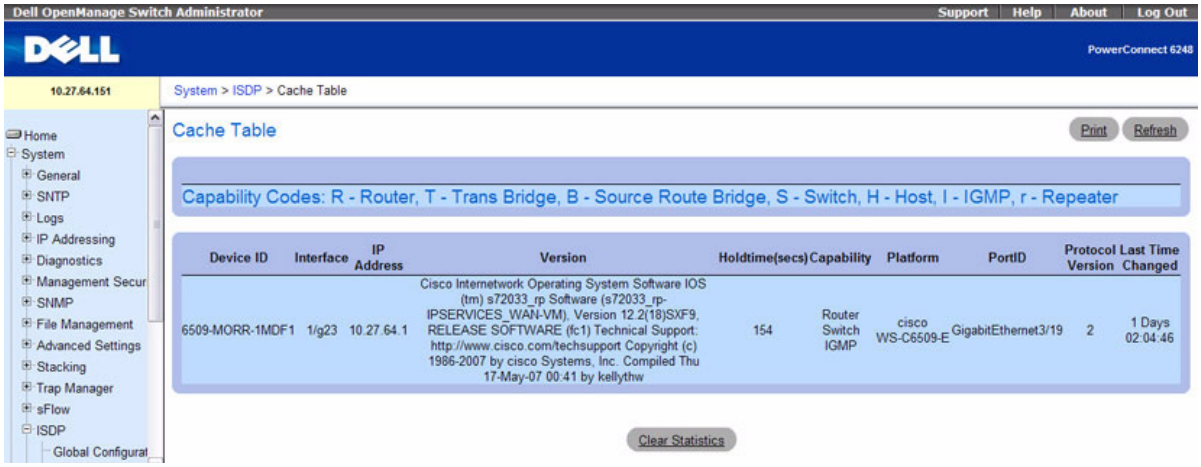
- ISDP Commands.

Cache Table

From the **ISDP Cache Table** page, you can view information about other devices the switch has discovered through the ISDP.

To access the **ISDP Cache Table** page, click **System > ISDP > Cache Table** in the navigation tree.

Figure 6-128. ISDP Cache Table



The **ISDP Cache Table** page contain the following fields:

- **Device ID** — Displays the string with Device ID which is reported in the most recent ISDP message.
- **Interface** — Displays the interface that this neighbor is attached to.
- **IP Address** — The (first) network-layer address that is reported in the Address TLV of the most recently received ISDP message.
- **Version** — Displays the Version string for the neighbor.
- **Holdtime** — Displays the ISDP holdtime for the neighbor.
- **Capability** — Displays the ISDP Functional Capabilities for the neighbor.
- **Platform** — Displays the ISDP Hardware Platform for the neighbor.
- **Port ID** — Displays the ISDP port ID string for the neighbor.

Downloaded from www.Manualslib.com manuals search engine

- **Protocol Version** — Displays the ISDP Protocol Version for the neighbor.
- **Last Time Changed** — Displays when entry was last modified.

Viewing ISDP Cache Table Information CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- ISDP Commands.

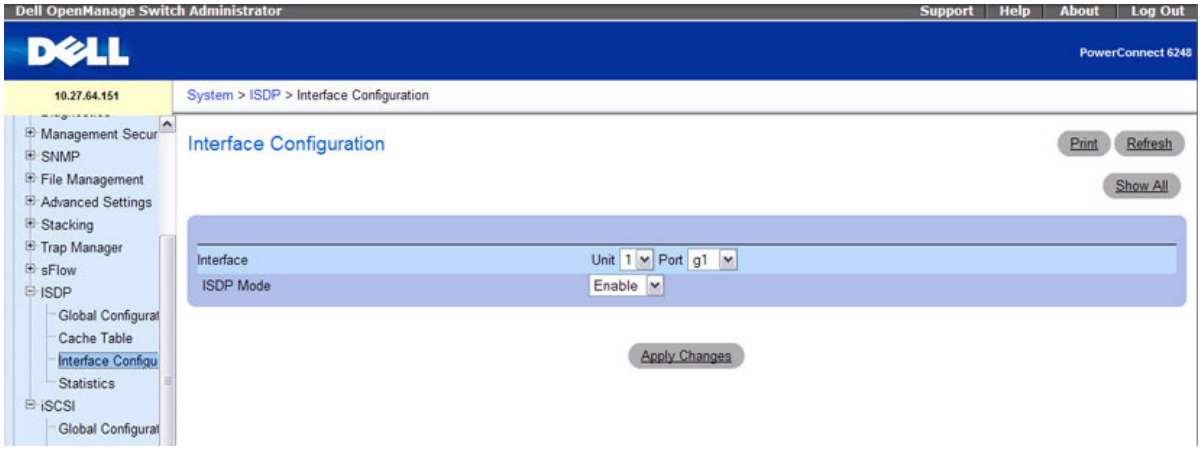
Interface Configuration

From the **ISDP Interface Configuration** page, you can configure the ISDP settings for each interface.

If ISDP is enabled on an interface, it must also be enabled globally in order for the interface to transmit ISDP packets. If the ISDP mode on the ISDP Global Configuration page is disabled, the interface will not transmit ISDP packets, regardless of the mode configured on the interface.

To access the **ISDP Interface Configuration** page, click **System > ISDP > Interface Configuration** in the navigation tree.

Figure 6-129. ISDP Interface Configuration



The **ISDP Interface Configuration** page contain the following fields:

- **Interface** — Select the interface with the ISDP mode status to configure or view.
- **ISDP Mode** — Use this field to enable or disable the Industry Standard Discovery Protocol on the selected interface.

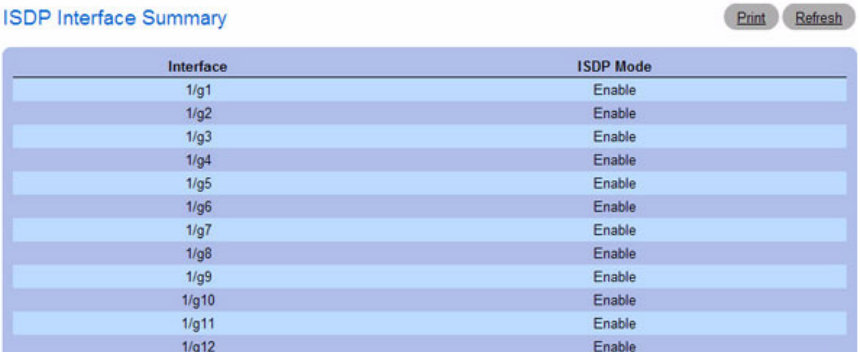
Displaying the ISDP Interface Summary Table

1. Open the **ISDP Interface Configuration** page.
2. Click **Show All**.

   The **ISDP Interface Summary** page displays:

Downloaded from www.Manualslib.com manuals search engine

Figure 6-130. ISDP Interface Summary



ISDP Interface Summary

Print Refresh

Interface	ISDP Mode
1/g1	Enable
1/g2	Enable
1/g3	Enable
1/g4	Enable
1/g5	Enable
1/g6	Enable
1/g7	Enable
1/g8	Enable
1/g9	Enable
1/g10	Enable
1/g11	Enable
1/g12	Enable

Configuring ISDP Using CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

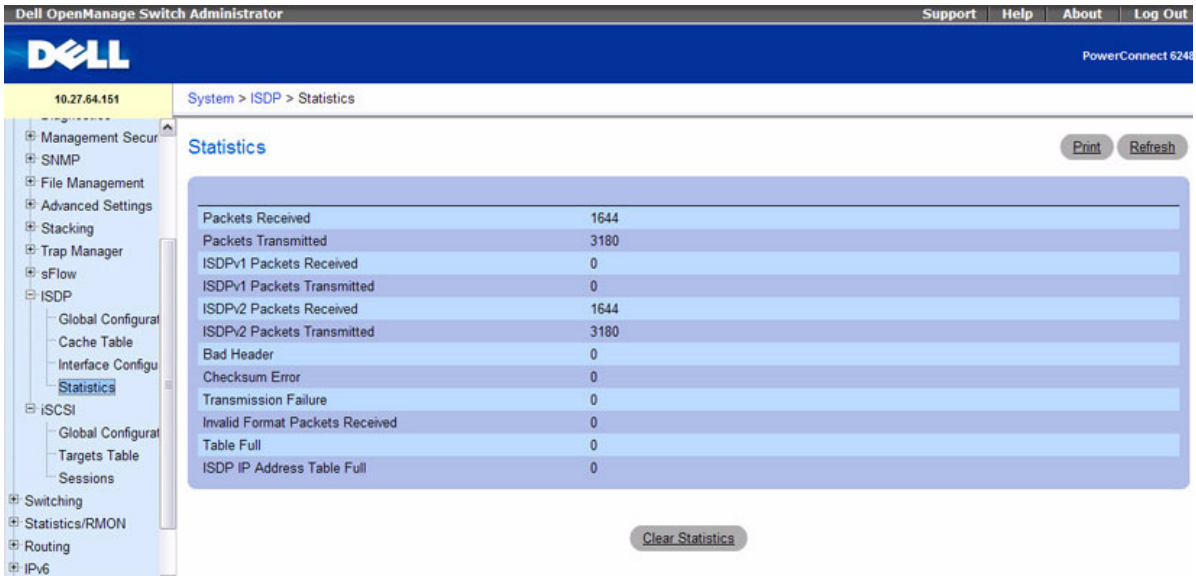
- ISDP Commands.

ISDP Statistics

From the **ISDP Statistics** page, you can view information about the ISDP packets sent and received by the switch.

To access the **ISDP Statistics** page, click **System** > **ISDP** > **Statistics** in the navigation tree.

Figure 6-131. ISDP Statistics



Downloaded from www.Manualslib.com manuals search engine

The **ISDP Statistics** page contain the following fields:

- **Packets Received** — Displays the number of all ISDP protocol data units (PDUs) received.
- **Packets Transmitted** — Displays the number of all ISDP PDUs transmitted.
- **ISDPv1 Packets Received** — Displays the number of v1 ISDP PDUs received.
- **ISDPv1 Packets Transmitted** — Displays the number of v1 ISDP PDUs transmitted.
- **ISDPv2 Packets Received** — Displays the number of v2 ISDP PDUs received.
- **ISDPv2 Packets Transmitted** — Displays the number of v2 ISDP PDUs transmitted.
- **Bad Header** — Displays the number of ISDP PDUs that were received with bad headers.
- **Checksum Error** — Displays the number of ISDP PDUs that were received with checksum errors.
- **Transmission Failure** — Displays the number of ISDP PDUs transmission failures.
- **Invalid Format Packets Received** — Displays the number of ISDP PDUs that were received with an invalid format.
- **Table Full** — Displays the number of times the system tried to add an entry to the ISDP table but was unsuccessful because the table was full.
- **ISDP IP Address Table Full** — Displays the number of times the system tried to add an entry to the ISDP IP Address table but was unsuccessful because the table was full.

Viewing ISDP Statistics Using CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- ISDP Commands.

Downloaded from www.Manualslib.com manuals search engine

7

Configuring Switching Information

Overview

This section provides all system operations and general information for network security, ports, address tables, GARP, VLANs, Spanning Tree, Port Aggregation, and Multicast Support.

The **Switching** menu page contains links to the following features:

- Configuring Network Security
- Configuring Ports
- Configuring Traffic Mirroring
- Configuring Address Tables
- Configuring GARP
- Configuring the Spanning Tree Protocol
- Configuring VLANs
- Configuring Voice VLAN
- Aggregating Ports
- Managing Multicast Support
- Configuring the Link Layer Discovery Protocol (LLDP)
- Creating Link Dependencies
- Dynamic ARP Inspection
- DHCP Snooping
- DHCP Relay
- Using the Port Aggregator Feature

Downloaded from www.Manualslib.com manuals search engine

Configuring Network Security

Use the **Network Security** menu page to set network security through port-based authentication, locked ports, DHCP Filtering configuration, and access control lists.

To display the **Network Security** page, click **Switching > Network Security** in the tree view.

The **Network Security** menu page contains links to the following features:

- Dot1x Authentication
- Authenticated Users
- Port Security
- IP ACL Configuration
- MAC ACL Configuration
- IPv6 Access Control Lists
- ACL Bind Configuration

Dot1x Authentication

IEEE 802.1X port-based network access control configuration is performed on the **Dot1x Authentication** page. MAC-based authentication allows multiple supplicants connected to the same port to each authenticate individually. For example, a system attached to the port might be required to authenticate in order to gain access to the network, while a VoIP phone might not need to authenticate in order to send voice traffic through the port.

The 802.1X network has three components:

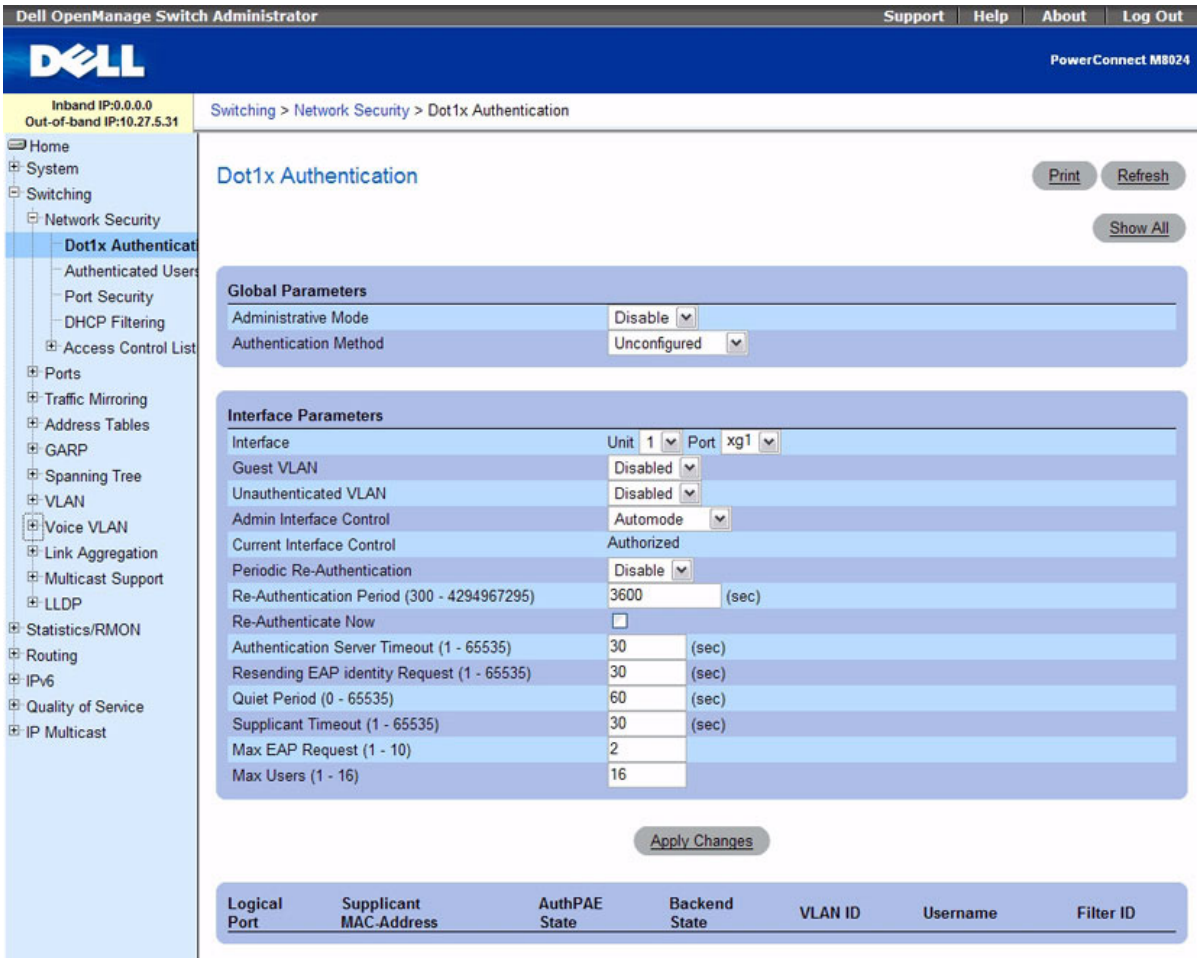
- **Authenticators** — Specifies the port that is authenticated before permitting system access.
- **Supplicants** — Specifies host connected to the authenticated port requesting access to the system services.
- **Authentication Server** — Specifies the external server, for example, the RADIUS server that performs the authentication on behalf of the authenticator, and indicates whether the user is authorized to access system services.

Use the **Dot1x Authentication** page to configure the 802.1X administrative mode on the switch and to configure general 802.1X parameters for a port.

To display the **Dot1x Authentication** page, click **Switching > Network Security > Dot1x Authentication** in the tree view.

Downloaded from www.Manualslib.com manuals search engine

Figure 7-1. Dot1x Authentication



The **Dot1x Authentication** page contains the following fields:

Global Parameters

- **Administrative Mode**— Permits 802.1X port-based authentication on the switch. The possible field values are:
  - **Enable** — Enables 802.1X authentication on the switch.
  - **Disable** — Disables 802.1X authentication on the switch.
- **Authentication Method** — Selects the Authentication method used. The possible field values are:
  - **Unconfigured** — Indicates that an authentication method has not been selected.
  - **None** — Indicates that no authentication method is used.
  - **RADIUS** — Indicates that authentication occurs at the RADIUS server.

Downloaded from www.Manualslib.com manuals search engine

Interface Parameters

- **Interface** — Selects the Unit and Port to be affected.
- **Guest VLAN** — Enables or disables the guest VLAN mode on this interface. To enable the guest VLAN, select the VLAN ID to use as the guest VLAN. All VLANs configured on the system are included in the menu.
- **Unauthenticated VLAN** — Allows or prohibits unauthenticated traffic on the port. To allow unauthenticated traffic on the port, select the ID of the VLAN to assign to supplicants that fail 802.1X authentication.
- **Admin Interface Control** — Defines the port authorization state. The possible field values are:
  - **Automode** — Automatically detects the mode of the interface.
  - **Authorized —** Places the interface into an authorized state without being authenticated. The interface sends and receives normal traffic without client port-based authentication.
  - **Unauthorized —** Denies the selected interface system access by moving the interface into unauthorized state. The switch cannot provide authentication services to the client through the interface.
  - **MAC-based** — Allows multiple hosts to authenticate on the interface. The hosts are distinguished by their MAC addresses.
- **Current Interface Control** — Displays the current port authorization state.
- **Periodic Re-Authentication** — Reauthenticates the selected port periodically, when enabled.
- **Re-Authentication Period** — Indicates the time span in which the selected port is reauthenticated. The possible field range is 300–4294967295 seconds. The field default is 3600 seconds.
- **Re-Authenticate Now** — Forces immediate port reauthentication, when selected.
- **Authentication Server Timeout** — Defines the amount of time that lapses before the switch resends a request to the authentication server. The possible field range is 1–65535 seconds. The field default is 30 seconds.
- **Resending EAP Identity Request** — Defines the amount of time that lapses before EAP requests are resent. The possible field range is 1–65535 seconds. The field default is 30 seconds.
- **Quiet Period** — Defines the amount of time that the switch remains in the quiet state following a failed authentication exchange. The possible field range is 0–65535 seconds. The field default is 60 seconds.
- **Supplicant Timeout** — Defines the amount of time that lapses before EAP requests are resent to the user. The possible field range is 1–65535 seconds. The field default is 30 seconds.
- **Max EAP Requests** — Defines the maximum number of times the switch can send an EAP request before restarting the authentication process if it does not receive a response. The possible field range is 1–10. The field default is 2 retries.

Downloaded from www.Manualslib.com manuals search engine

- **Max Users** — Set the maximum number of clients supported on the port when MAC-based 802.1X authentication is enabled on the port. The number of users allowed to authenticate per port ranges from 1 to 16.
- **Termination Cause** — Displays the reason for termination.
- **MAC Authentication Bypass** — Enable this feature to provide 802.1x unaware clients controlled access to the network using the MAC address of the device as an identifier. The known and allowable MAC address and corresponding access rights must be configured in the authentication server. MAC Authentication Bypass only works when the port control mode of the port is MAC based.
- When supplicants connect to the port, information about that supplicant is displayed in a table below the configuration fields. The supplicant table contains the following information:
- **Logical Port** — The port to which the supplicant is connected.
- **Supplicant MAC Address** — The MAC-address of the supplicant
- **Authenticator PAE** — Current state of the authenticator PAE state machine. Possible values are Initialize, Disconnected, Connecting, Authenticating, Authenticated, Aborting, Held, ForceAuthorized, and ForceUnauthorized.
- **Backend PAE** — Current state of the backend authentication state machine. Possible values are Request, Response, Success, Fail, Timeout, Idle, and Initialize.
- **VLAN Assigned** — The VLAN assigned to the client by the RADIUS server. When VLAN assignments are disabled, the RADIUS server does not assign any VLAN to the port, and this field is set to 0.
- **Username** — The username representing the identity of the Supplicant. This field shows the username when the Admin Interface Control is Automode or MAC-based. If the port is Authorized, it shows the username of the current user. If the port is unauthorized it shows the last user that was authenticated successfully.
- **Filter ID** — The Filter Id assigned to the client by the RADIUS server. This field is not applicable when the Filter-Id feature is disabled on the RADIUS server and client.

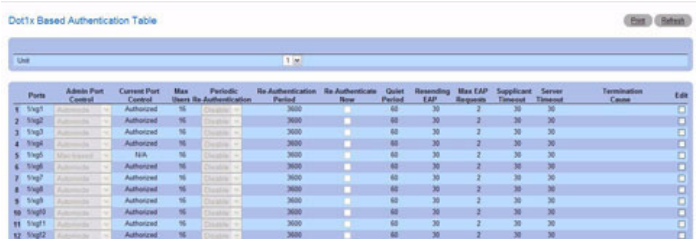
Displaying the Dot1x Authentication Table

1. Open the **Dot1x Authentication** page.
2. Click **Show All**.

   The **Dot1x Authentication Table** page opens, displaying the left side of the table:

Downloaded from www.Manualslib.com manuals search engine

Figure 7-2. Dot1x Authentication Table



3. Use the horizontal scroll bar or click the right arrow at the bottom of the screen to display the right side of the table.
4. Use the **Unit** drop-down menu to view the **Dot1x Authentication Table** for other units in the stack, if they exist.

Re-Authenticating One Port

1. Open the **Dot1x Authentication** page.
2. Click **Show All**.

   The **Dot1x Authentication Table** displays.
3. Check **Edit** to select the Unit/Port to re-authenticate.
4. Check **Reauthenticate Now**.
5. Click **Apply Changes**.

   The specified port is re-authenticated, and the device is updated.

Re-Authenticating Multiple Ports in the Dot1x Authentication Table

1. Open the **Dot1x Authentication** page.
2. Click **Show All**.

   The **Dot1x Authentication Table** displays.
3. Check **Edit** to select the Units/Ports to re-authenticate.
4. To re-authenticate on a periodic basis, set **Periodic Re-Authentication** to Enable, and specify a **Re-Authentication Period** for all desired ports.
5. To re-authenticate immediately, check **Reauthenticate Now** for all ports to be re-authenticated.
6. Click **Apply Changes**.

   Specified ports are re-authenticated (either immediately or periodically), and the device is updated.

Downloaded from www.Manualslib.com manuals search engine

Changing Administrative Port Control

1. Open the **Dot1x Authentication** page.
2. Click **Show All**.

   The **Dot1x Authentication Table** displays.
3. Scroll to the right side of the table and select the **Edit** check box for each port to configure. Change **Admin Port Control** to **Authorized**, **Unauthorized**, or **Automode** as needed for chosen ports. Only **MAC-Based** and **Automode** actually uses dot1x to authenticate. **Authorized** and **Unauthorized** are manual overrides.
4. Click **Apply Changes**.

   Admin Port Control is updated for the specified ports, and the device is updated.

Enabling Dot1x Authentication Using the CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

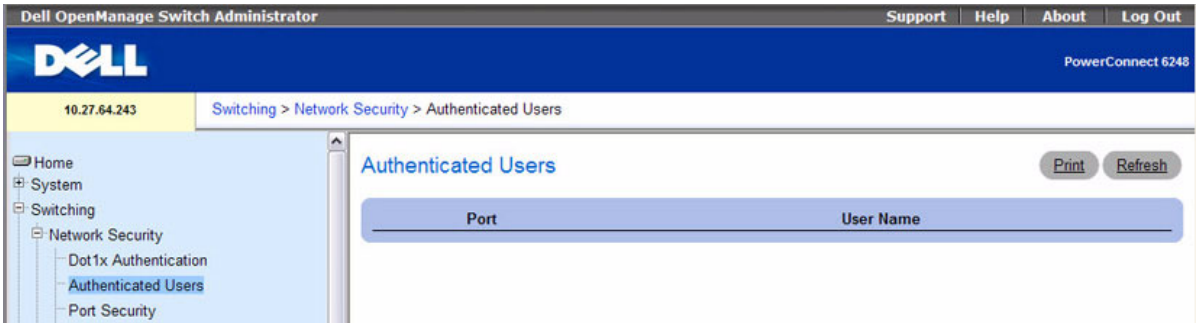
- 802.1X Commands

Authenticated Users

The **Authenticated Users** page is used to display lists of ports that have authenticated users.

To display the **Authenticated Users** page, click **Switching** > **Network Security** > **Authenticated Users** in the tree view.

Figure 7-3. Network Security Authenticated Users



The **Authenticated Users** page contains the following fields:

- **Port** — Displays the port used for authentication.
- **User Name** — Specifies a user from the list of users authorized via the RADIUS Server.

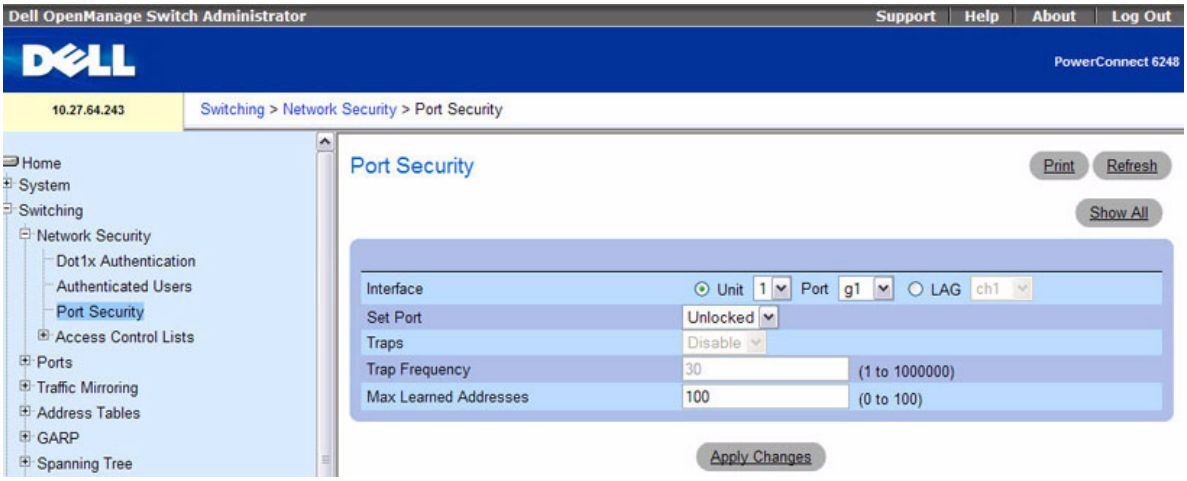
Downloaded from www.Manualslib.com manuals search engine

Port Security

The **Port Security** page is used to enable security on a per-port basis. When a port is locked, only packets with allowable source MAC addresses can be forwarded. All other packets are discarded. A MAC address can be defined as allowable by one of two methods: dynamically or statically.

To display the **Port Security** page, click **Switching** > **Network Security** > **Port Security** in the tree view.

Figure 7-4. Network Security Port Security



The **Port Security** page contains the following fields:

- **Interface** — Displays the unit and port or the LAG on which the locked port security is enabled.
- **Set Port** — Enables locking the port or LAG. When a port is locked, all the current addresses that had been dynamically learned by the switch on that port are removed from the list. When the port is unlocked, they are removed from the static list.
- **Traps** — Enables or disables sending a trap when a packet is received on a locked port or LAG.
- **Trap Frequency** — Specifies the time interval in seconds between successive traps. The valid range is 1 to 1000000 seconds.
- **Max Learned Addresses** — Specifies the Max Learned Addresses count. Valid range is 0 to 100.

Defining a Locked Port

1. Open the **Port Security** page.
2. Select an interface type and number.
3. Select **Locked** on the **Set Port** drop-down menu.
4. Complete the remaining fields.
5. Click **Apply Changes**.

   The locked port/LAG is added to the Port Security table, and the device is updated.

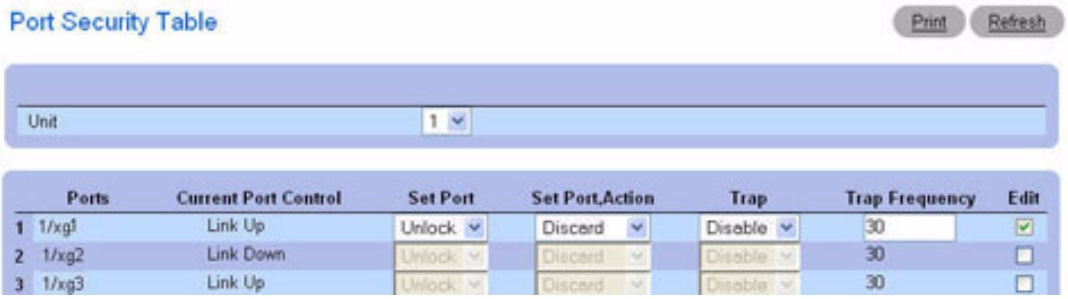
Downloaded from www.Manualslib.com manuals search engine

Viewing the Port Security Table

1. Open the **Port Security** page.
2. Click **Show All.**

   The **Port Security Table** displays.

Figure 7-5. Port Security Table



3. Use the **Unit** drop-down menu to view the **Port Security Table** for other units in the stack, if they exist.

Defining Multiple Locked Ports

1. Open the **Port Security** page.
2. Click **Show All.**

   The **Port Security Table** displays.
3. Click **Edit** for each port whose parameters are to be changed.
4. Fields can now be edited as needed for these ports.
5. Click **Apply Changes**.

   The changes are made to the Port Security table, and the device is updated.

Configuring Port Security with CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- Address Table Commands

IP ACL Configuration

Access control lists (ACL) allow network managers to define classification actions and rules for specific ingress ports. Your switch supports up to 100 ACLs. However, the hardware resources are limited and may not be able to fully support 100 completely populated ACLs.

Downloaded from www.Manualslib.com manuals search engine

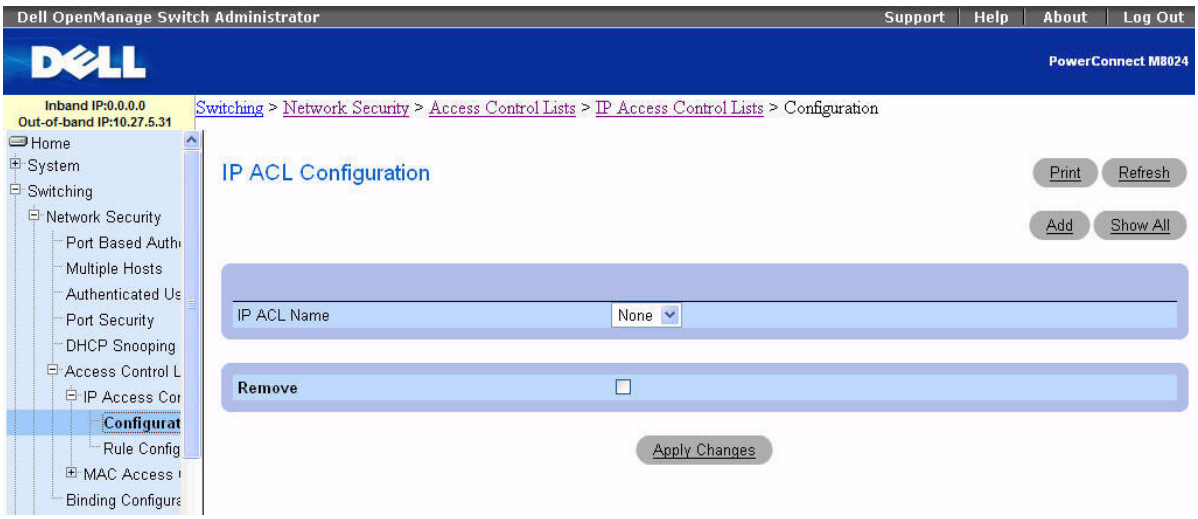
Packets can be filtered on ingress or egress. If the filter rules match, then some actions can be taken, including dropping the packet or disabling the port. For example, a network administrator defines an ACL rule that says port number 20 can receive TCP packets. However, if a UDP packet is received the packet is dropped.

ACLs are composed of access control entries (ACE), or rules, that consist of the filters that determine traffic classifications. The total number of rules that can be defined for each ACL is 127.

Use the **IP ACL Configuration** page to add or remove IP-based ACLs.

To display the **IP ACL Configuration** page, click **Switching > Network Security > Access Control Lists > IP Access Control Lists > Configuration** in the tree view.

Figure 7-6. IP ACL Configuration



The **IP ACL Configuration** page contains the following fields:

- **IP ACL Name** — Specifies user-defined name for the ACL.
- **Remove** — Removes the IP ACL selected in the IP ACL field.

Adding an IP-based ACL

1. Open the **IP ACL Configuration** page.
2. Click **Add**.

   The **Add IP ACL** page displays.

Downloaded from www.Manualslib.com manuals search engine

Figure 7-7. Add IP ACL

3. Enter the desired **ACL Name** in the related entry field.
4. Click **Apply Changes**.

   The IP-based ACL is added, and the device is updated.

Removing an IP-based ACL

1. Open the **IP ACL Configuration** page, and select the ACL to be deleted from the **IP ACL** drop-down menu.
2. Check the **Remove** ACL check box.
3. Click **Apply Changes**.

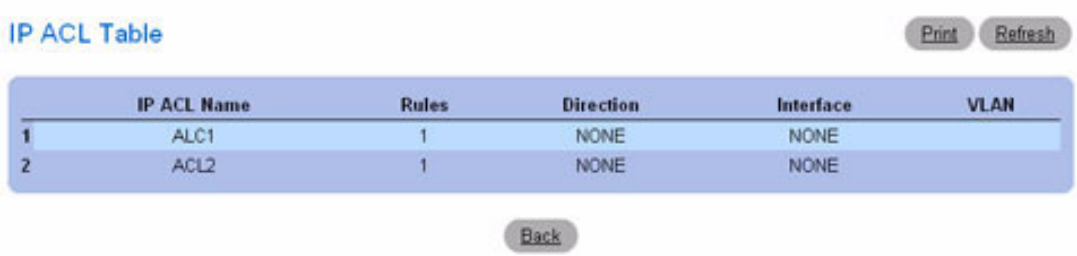
   The IP-based ACL is removed, and the device is updated.

Displaying IP ACLs

1. Open the **IP ACL Configuration** page.
2. Click **Show All**.

   All IP ACLs and their related data display in the **IP ACL Table**.

Figure 7-8. IP ACL Table



Adding an IP-based ACL Using the CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- ACL Commands

Downloaded from www.Manualslib.com manuals search engine

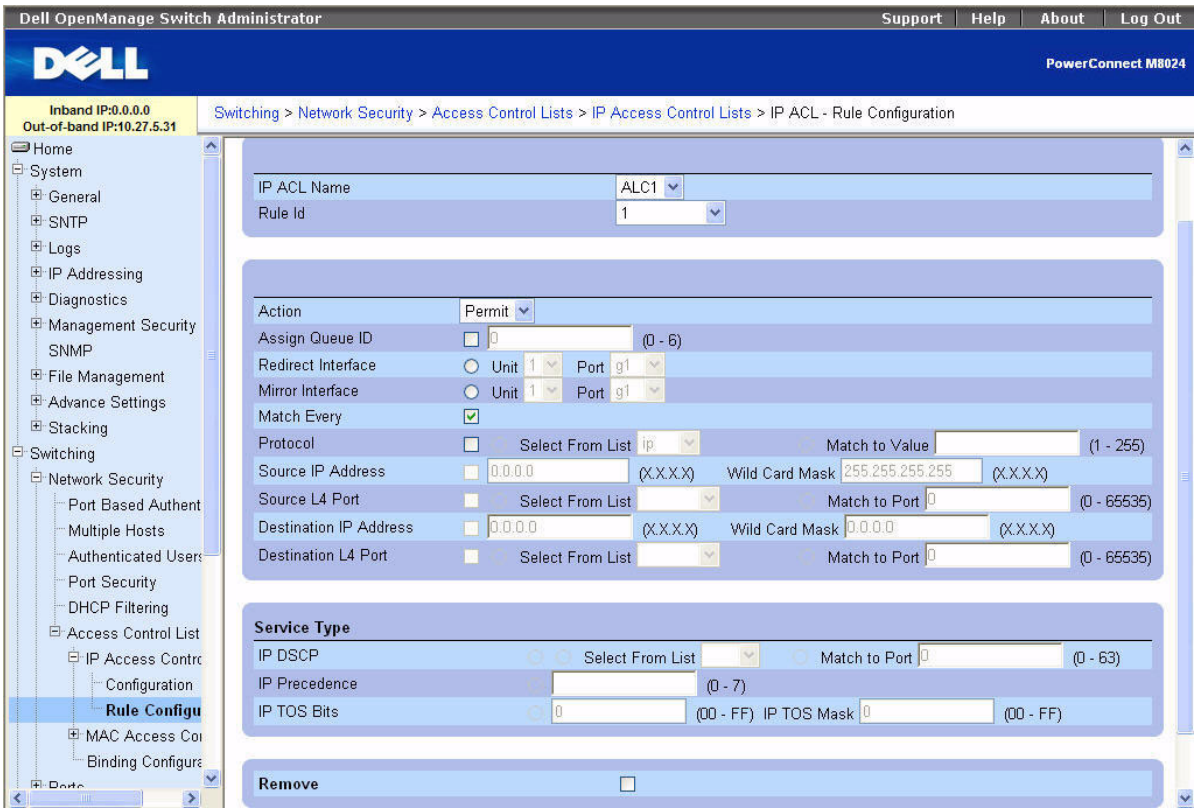
IP ACL Rule Configuration

Use the **IP ACL Rule Configuration** page to define rules for IP-based ACLs. The access list definition includes rules that specify whether traffic matching the criteria is forwarded normally or discarded. Additionally, you can specify to assign traffic to a particular queue, filter on some traffic, change VLAN tag, shut down a port, and/or redirect the traffic to a particular port.

NOTE: There is an implicit "deny all" rule at the end of an ACL list. This means that if an ACL is applied to a packet and if none of the explicit rules match, then the final implicit "deny all" rule applies and the packet is dropped.

To display the **IP ACL Rule Configuration** page, click **Switching > Network Security > Access Control Lists > IP Access Control Lists > Rule Configuration** in the tree view.

Figure 7-9. IP ACL - Rule Configuration (Standard)



The **IP ACL Rule Configuration** page contains the following fields:

- **IP ACL Name** — Specifies an existing IP ACL. To set up a new IP ACL use the "IP ACL Configuration" page.
- **Rule ID** — Selects or creates user-defined ACLs. Enter an existing Rule ID, or create a new one by selecting Create from the drop-down menu and entering the desired new Rule ID in the field next to it. The new ID is created once Apply Changes is clicked. Up to 127 rules can be created for each ACL.

Downloaded from www.Manualslib.com manuals search engine

- **Action** — Selects the ACL forwarding action. Choose from the drop-down menu options to apply a forwarding action. Possible values are:
  - **Permit** — Forwards packets which meet the ACL criteria.
  - **Deny** — Drops packets which meet the ACL criteria.
- **Assign Queue ID** — Click the check box to apply this criteria, then enter an identifying number from 0 to 6.
- **Redirect Interface** — Select from the drop-down list of interfaces one that packets meeting this rule can be redirected to.
- **Mirror Interface** — Select from the drop-down list of interfaces one that packets meeting this rule can be mirrored to.
- **Logging** — Enables logging for a particular ACL when the check box is selected. Logging is supported for Deny action only.
- **Match Every** — Requires a packet to match the criteria of this ACL. Click the check box to apply this criteria. Match Every is exclusive to the other filtering rules, so if checked, the other rules on the screen aren't accessible.
- **Protocol** — Requires a packet's protocol to match the protocol listed here. Click the check box to apply this criteria, then select one of the following:
  - **Select from List** — Select from the drop-down list of protocols on which the rule can be based.
  - **Match to Value** — Click to add a user-defined Protocol ID used to match packets to the rule.
- **Source IP Address** — Requires a packet's source port IP address to match the address listed here. Click the check box and enter an address to apply this criteria.
- **Wild Card Mask** — Specifies the source IP address wildcard mask. Wild card masks determines which bits are used and which bits are ignored. A wild card mask of 255.255.255.255 indicates that no bit is important. A wildcard of 0.0.0.0 indicates that all of the bits are important. This field is required when **Source IP Address** is checked.
- **Source L4 Port** — Requires a packet's TCP/UDP source port to match the port listed here. Click the check box to apply this criteria, then select one of the following from the drop-down menu:
  - **Select From List** — Click to select from a list of source ports on which the rule can be based.
  - **Match to Port** — Click to add a user-defined Port ID by which packets are matched to the rule.
- **Destination IP Address** — Requires a packet's destination port IP address to match the address listed here. Click the check box and enter an address to apply this criteria.
- **Wild Card Mask** — Specifies the Destination IP address wildcard mask. This field is required when **Destination IP Address** is checked.
- **Destination L4 Port** — Requires a packet's TCP/UDP destination port to match the port listed here. Click the check box to apply this criteria, then select one of the following:
  - **Select From List** — Select from a list of destination ports on which the rule can be based.
  - **Match to Port** — Click to add a user-defined Port ID by which packets are matched to the rule.

Downloaded from www.Manualslib.com manuals search engine

Service Type fields

Select one of the following three Match fields to use in matching packets to ACLs:

- **IP DSCP** — Matches the packet DSCP value to the rule. Either the DSCP value or the IP Precedence value is used to match packets to ACLs.
  - **Select From List** — Select from a list of DSCP keyword values.
  - **Match to Port** — Click to add a user-defined Port ID.
- **IP Precedence** — Matches the packet IP Precedence value to the rule when checked. Enter the IP Precedence value to match. Either the DSCP value or the IP Precedence value is used to match packets to ACLs.
- **IP TOS Bits** — Matches on the Type of Service bits in the IP header when checked.
  - **TOS Bits** — Requires the bits in a packet's TOS field to match the two-digit hexadecimal number entered here.
  - **TOS Mask** — Specifies the bit positions used for comparison against the IP TOS field in a packet.
- **Remove** — Removes a Rule ID when **Remove** is checked and **Apply Changes** is clicked.

Modifying an IP-based Rule

NOTE: Rules can be modified only when the ACL to which they belong is not bound to an interface.

1. Open the **IP ACL Rule Configuration** page.
2. Select the desired ACL from the **IP ACL** drop-down menu.
3. Select the desired rule from the **Rule ID** drop-down menu.
4. Modify the remaining fields as needed.
5. Click **Apply Changes**.

   The IP-based rule is modified, and the device is updated.

Adding a New Rule to an IP-based ACL

1. Open the **IP ACL Rule Configuration** page.
2. Select the desired ACL from the **IP ACL** drop-down menu.
3. Select **Create Rule** from the **Rule ID** drop-down menu and enter a new ID number.
4. Define the remaining fields as needed.
5. Click **Apply Changes**.

   The new rule is assigned to the specified IP-based ACL.

Defining an IP-based ACL Rule Using the CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

Downloaded from www.Manualslib.com manuals search engine

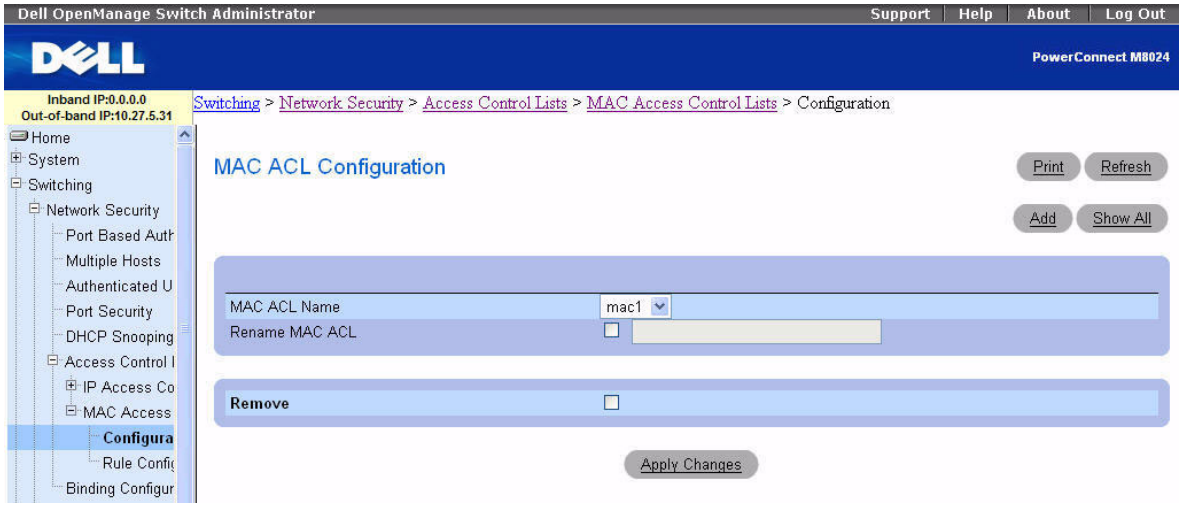
- ACL Commands

MAC ACL Configuration

The **MAC ACL Configuration** page allows network administrators to define a MAC-based ACL. For an explanation of ACLs, see "IP ACL Configuration."

To display the **MAC ACL Configuration** page, click **Switching > Network Security > Access Control Lists > MAC Access Control Lists > Configuration** in the tree view.

Figure 7-10. MAC ACL Configuration



The **MAC ACL Configuration** page contains the following fields:

- **MAC ACL Name** — User-defined ACL name.
- **Rename MAC ACL** — To rename the MAC ACL, select the check box and enter a new MAC ACL name in the field.
- **Remove** — Click this field, then click the Apply Changes button to delete the MAC ACL listed in the MAC ACL field.

Adding a MAC-based ACL

1. Open the **MAC ACL Configuration** page.
2. Click **Add** to display the **Add MAC ACL** page.

Downloaded from www.Manualslib.com manuals search engine

Figure 7-11. Add MAC ACL

3. Enter the desired MAC **ACL Name** in the entry field.
4. Click **Apply Changes**.

   The MAC-based ACL is added, and the device is updated.

Removing a MAC-based ACL

1. Open the **MAC ACL Configuration** page, and select the ACL to be removed from the **MAC ACL** drop-down menu.
2. Select the **Remove** check box.
3. Click **Apply Changes**.

   The MAC-based ACL is removed, and the device is updated.

Displaying MAC ACLs

1. Open the **MAC ACL Configuration** page.
2. Click **Show All**.

   All MAC ACLs and their related data are displayed on screen.

Figure 7-12. MAC ACL Table

Configuring MAC-based ACLs Using the CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- ACL Commands

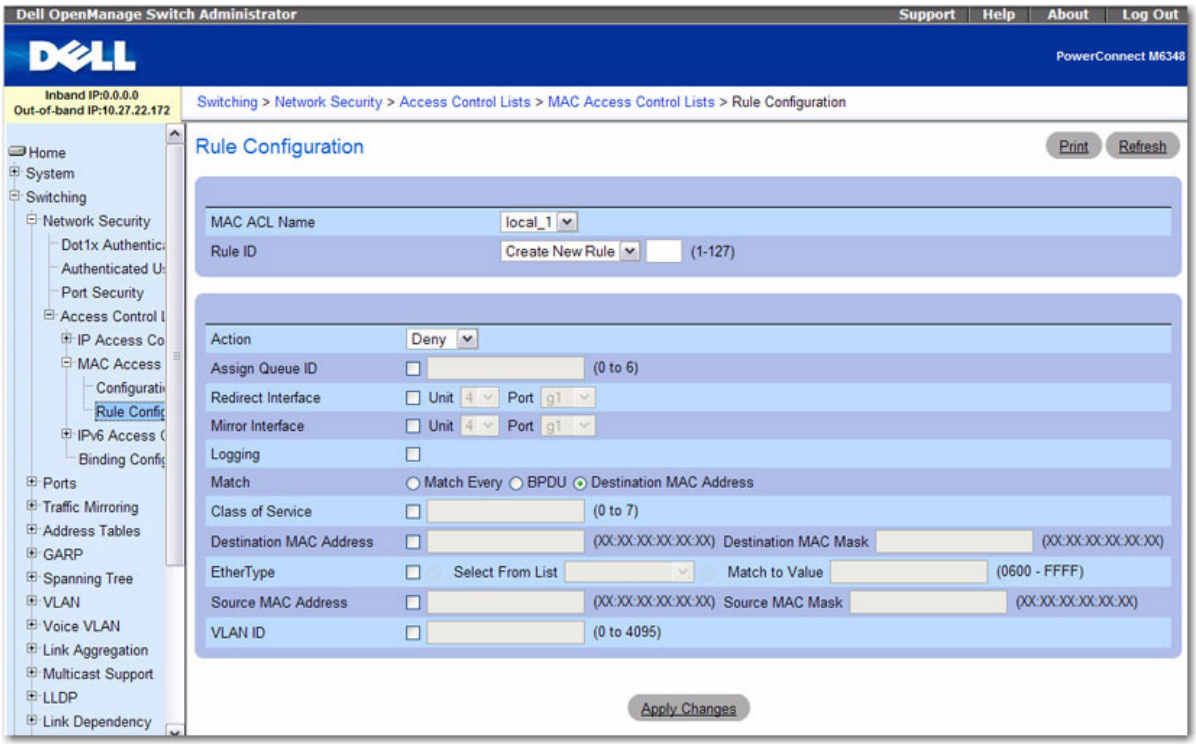
Downloaded from www.Manualslib.com manuals search engine

MAC ACL Rule Configuration

Use the **MAC ACL Rule Configuration** page to define rules for MAC-based ACLs. The access list definition includes rules that specify whether traffic matching the criteria is forwarded normally or discarded. A default 'deny all' rule is the last rule of every list.

To display the **MAC ACL Rule Configuration** page, click **Switching > Network Security > Access Control Lists > MAC Access Control Lists > Rule Configuration** in the tree view.

Figure 7-13. MAC ACL - Rule Configuration



The **MAC ACL Rule Configuration** page contains the following fields:

- **MAC ACL Name** — Specifies an existing MAC ACL. To set up a new MAC ACL use the MAC ACL Configuration page.
- **Rule Id** — Selects or creates a user-defined ACLs. Enter an existing Rule ID, or create a new one by selecting Create from the drop-down menu and entering the desired new Rule ID in the field next to it. The new ID is created once Apply Changes is clicked.
- **Action** — Selects the ACL forwarding action, which can be one of the following values:
  - **Permit** — Forwards packets which meet the ACL criteria.
  - **Deny** — Drops packets which meet the ACL criteria.

Downloaded from www.Manualslib.com manuals search engine

- **Assign Queue ID** — Click the check box to apply this criteria, then enter an identifying number from 0 to 6.
- **Redirect Interface** — Select from the drop-down list of interfaces one that packets meeting this rule can be redirected to.
- **Mirror Interface** — Select from the drop-down list of interfaces one that packets meeting this rule can be mirrored to.
- **Logging** — Click the check box to enable logging for this ACL. This feature is supported for the Deny action only.
- **Match Every** — Requires a packet to match the criteria of this ACL. Click the check box to apply this criteria.
- **Class of Service** — Requires a packet's CoS to match the CoS value listed here. Click the check box and enter a CoS value between 0 and 7 to apply this criteria.
- **Secondary CoS** — Requires a packet's secondary CoS to match the CoS value listed here. Click the check box and enter a CoS value between 0 and 7 to apply this criteria.
- **Destination MAC Address** — Requires a packet's destination port MAC address to match the address listed here. Click the check box and enter an address to apply this criteria.
- **Destination MAC Mask** — Enter the MAC Mask associated with the Destination MAC to match.
- **EtherType** — Requires a packet's EtherType to match the EtherType listed here. Click the check box and select from a list or enter the EtherType ID:
  - **Select from List** — Select desired EtherType from the drop-down menu.
  - **Match to Value** — Enter the desired port number to match.
- **Source MAC Address** — Requires a packet's source port MAC address to match the address listed here. Click the check box and enter an address to apply this criteria.
- **Source MAC Mask** — If desired, enter the MAC mask for the source MAC address to match.
- **Vlan Id** — Requires a packet's VLAN ID to match the ID listed here. Click the check box and enter the VLAN ID to apply this criteria. Possible field values are 1–4095.
- **Remove** — Removes the MAC ACL Rule when **Remove** is checked and **Apply Changes** is clicked.

Modifying a MAC-based Rule

Note: Rules can be modified only when the ACL to which they belong is not bound to an interface.

1. Open the **MAC ACL Rule Configuration** page.
2. Select the desired ACL from the **MAC ACL** drop-down menu.
3. Select the desired rule from the **Rule ID** drop-down menu.
4. Modify the remaining fields as needed.
5. Click **Apply Changes**.

   The MAC-based rule is modified, and the device is updated.

Downloaded from www.Manualslib.com manuals search engine

Adding a New Rule to a MAC-based ACL

1. Open the **MAC ACL Rule Configuration** page.
2. Select the desired ACL from the **MAC ACL** drop-down menu.
3. Specify **Create New Rule** for **Rule ID**.
4. Enter a new ID number.
5. Define the remaining fields as needed.
6. Click **Apply Changes**.

   The new rule is assigned to the specified MAC-based ACL.

Removing a Rule From a MAC-based ACL

1. Select an ACL.
2. Select a rule from the **Rule ID** drop-down menu.
3. Check the **Remove** check box.
4. Click **Apply Changes**.

   The MAC-based ACL is removed, and the device is updated.

Defining a MAC-based ACL Rule Using the CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- ACL Commands

IPv6 Access Control Lists

An IPv6 ACL consists of a set of rules which are matched sequentially against a packet. When a packet meets the match criteria of a rule, the specified rule action (Permit/Deny) is taken and the additional rules are not checked for a match. On this menu the interfaces to which an IPv6 ACL applies must be specified, as well as whether it applies to inbound or outbound traffic. Rules for the IPv6 ACL are specified/created using the IPv6 ACL Rule Configuration menu.

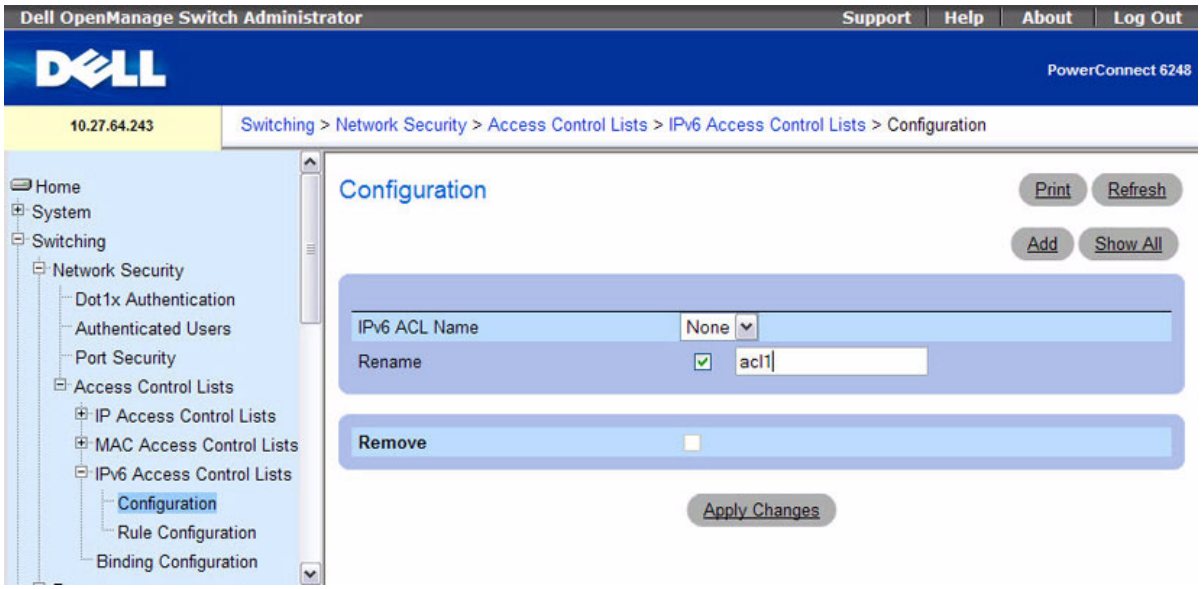
First, you use the **IPv6 ACL Configuration** page to define the IP ACL type and assign an ID to it. Then, you use the IPv6 ACL Rule Configuration page to create rules for the ACL. Finally, you use the ACL Interface Configuration and/or ACL Interface/VLAN Summary pages to assign the ACL by its ID number to a port or VLAN. You can use the **IPv6 ACL Table** page to view the configurations. See "Displaying IPv6 ACLs" on page 279.

IPv6 ACL Configuration

Use the **IPv6 ACL Configuration** page to add or remove IP-based ACLs. To display the IP ACL Configuration page, click **Switching > Network Security > Access Control Lists > IPv6 Access Control Lists > IPv6 ACL Configuration** in the tree view.

Downloaded from www.Manualslib.com manuals search engine

Figure 7-14. IPv6 ACL Configuration



The **IPv6 ACL Configuration** page contains the following fields:

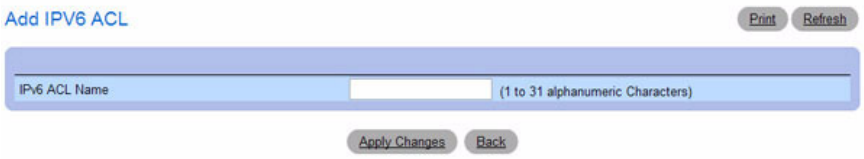
- **IPv6 ACL Name** — Specify an IPv6 ACL name string which includes alphanumeric characters only. The name must start with an alphabetic character. This field displays the name of the currently selected IPv6 ACL if any ACLs have already been created.
- **Rename** — To rename an existing IPv6 ACL, select this option, enter a new name in the text field, and click **Apply Changes**. The changes are applied to the ACL that is selected in the IPv6 ACL Name field.
- **Remove** — To remove an existing IPv6 ACL, select the ACL from the IPv6 ACL Name menu, select the remove option, and click **Apply Changes**.

Adding an IPv6-based ACL

1. Open the **IPv6 ACL Configuration** page.
2. Click **Add**.

   The **Add IPv6 ACL** page displays.

Figure 7-15. Add IPv6 ACL



3. Enter a name for the IPv6 ACL.

Downloaded from www.Manualslib.com manuals search engine

4. Click **Apply Changes**.

Displaying IPv6 ACLs

1. Open the **IPv6 ACL Configuration** page.
2. Click **Show All**.

   All IP ACLs and their related data display in the **IPv6 ACL Table**.

Figure 7-16. IPv6 ACL Table

The **Summary** page has the following fields:

- **IPv6 ACL Name** — Describes the number ranges for IPv4 ACL standard versus extended. The range for a standard IP ACL is 1-99. For an extended IP ACL, the ID range is 101-199.
- **Rules** — Shows the number of rules currently configured for the IP ACL.
- **Direction** — Shows the direction of packet traffic affected by the IP ACL, which can be Inbound or blank.
- **Interface** — Shows the interfaces to which the IP ACL applies.
- **VLAN ID** — The VLAN(s) to which the IPv6 ACL applies.

Configuring an IPv6 ACL by Using the CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- ACL Commands

IPv6 ACL Rule Configuration

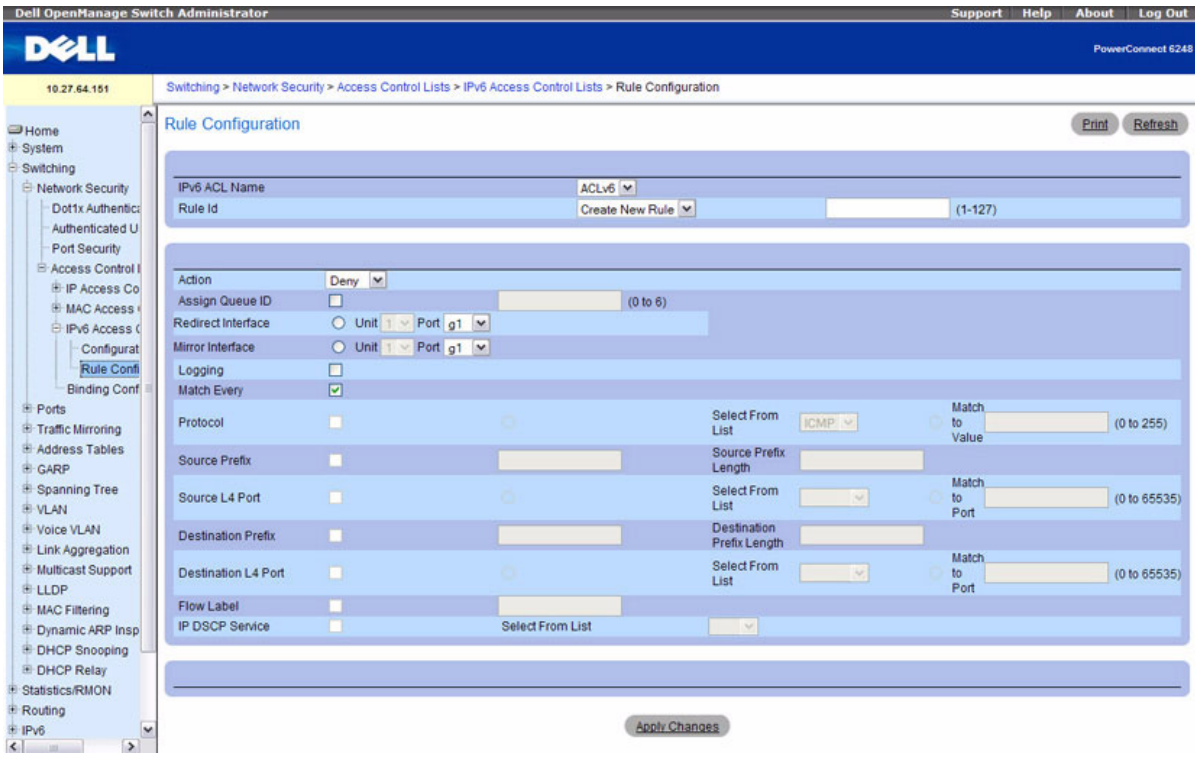
Use the IPv6 ACL Rule Configuration page to define rules for IPv6-based ACLs. The access list definition includes rules that specify whether traffic matching the criteria is forwarded normally or discarded. Additionally, you can specify to assign traffic to a particular queue, filter on some traffic, change VLAN tag, shut down a port, and/or redirect the traffic to a particular port. By default, no specific value is in effect for any of the IPv6 ACL rules.

There is an implicit “deny all” rule at the end of an ACL list. This means that if an ACL is applied to a packet and if none of the explicit rules match, then the final implicit “deny all” rule applies and the packet is dropped.

Downloaded from www.Manualslib.com manuals search engine

To display the IPv6 ACL Rule Configuration page, click **Switching > Network Security > Access Control Lists > IPv6 Access Control Lists > Rule Configuration** in the navigation menu.

Figure 7-17. IPv6 ACL - Rule Configuration



The **IPv6 ACL Configuration** page contains the following fields:

- **IPv6 ACL Name** — Select the ACL you want to configure.
- **Rule ID** — Select an existing Rule ID to modify or select Create Rule to configure a new ACL Rule. To create a new rule, enter a rule ID from 1–127 in the available field. New rules cannot be created if the maximum number of rules has been reached. For each rule, a packet must match all the specified criteria in order to be true against that rule and for the specified rule action (Permit/Deny) to take place.
- **Action** — Specify what action should be taken if a packet matches the rule's criteria. The choices are Permit or Deny.
- **Assign Queue ID** — Specifies the hardware egress queue identifier used to handle all packets matching this IPv6 ACL rule. Valid range of Queue IDs is 0 to 6.
- **Redirect Interface** — Specifies the egress interface where the matching traffic stream is forced, bypassing any forwarding decision normally performed by the device. This field cannot be set if a Mirror Interface is already configured for the ACL rule.

Downloaded from www.Manualslib.com manuals search engine

- **Mirror Interface** — Specifies the egress interface where the matching traffic stream is copied, in addition to it being forwarded normally by the device. This field cannot be set if a Redirect Interface is already configured for the ACL rule.
- **Logging** — When set to True, logging is enabled for this ACL rule (subject to resource availability in the device). If the Access List Trap Flag is also enabled, this will cause periodic traps to be generated indicating the number of times this rule was activated during the current report interval. A fixed 5 minute report interval is used for the entire system. A trap is not issued if the ACL rule hit count is zero for the current interval. This field is visible for a Deny action.
- **Match Every** — Select True or False from the menu.
- True signifies that all packets will match the selected IPv6 ACL and rule and will be either permitted or denied. In this case, since all packets match the rule, the option of configuring other match criteria will not be offered. To configure specific match criteria for the rule, remove the rule and re-create it, or re-configure 'Match Every' to 'False' for the other match criteria to be visible.
- **Protocol** — There are two ways to configure IPv6 protocol.
  - Specify an integer ranging from 1 to 255 after selecting protocol keyword “other”. This number represents the IP protocol.
  - Select name of a protocol from the existing list of Internet Protocol (IP), Transmission Control Protocol (TCP), User Datagram Protocol (UDP), Internet Control Message Protocol (ICMP) and Internet Group Management Protocol (IGMP).
- **Source Prefix/PrefixLength** — Specify IPv6 Prefix combined with IPv6 Prefix length of the network or host from which the packet is being sent. Prefix length can be in the range (0 to 128).
- **Source L4 Port** — Specify a packet's source layer 4 port as a match condition for the selected IPv6 ACL rule. Source port information is optional. Source port information can be specified in two ways:
  - Select keyword “other” from the drop down menu and specify the number of the port in the range from 0 to 65535.
  - Select one of the keyword from the list: DOMAIN, ECHO, FTP, FTPDATA, HTTP, SMTP, SNMP, TELNET, TFTP, and WWW. Each of these values translates into its equivalent port number, which is used as both the start and end of the port range.
- **Destination Prefix/Prefix Length** — Enter up to a 128-bit prefix combined with the prefix length to be compared to a packet's destination IP address as a match criteria for the selected IPv6 ACL rule. The prefix length can be in the range 0 to 128.
- **Destination L4 Port Number** — Specify a packet's destination layer 4 port number match condition for the selected IPv6 ACL rule. This is an optional configuration.
- **Destination L4 Port Keyword** — Specify the destination layer 4 port match conditions for the selected IPv6 ACL rule. The possible values are DOMAIN, ECHO, FTP, FTPDATA, HTTP, SMTP, SNMP, TELNET, TFTP, and WWW. Each of these values translates into its equivalent port number, which is used as both the start and end of the port range. This is an optional configuration.
- **Flow Label** — A 20-bit number that is unique to an IPv6 packet that is used by end stations to signify QoS handling in routers. The flow label can specified within the range 0 to 1048575.

Downloaded from www.Manualslib.com manuals search engine

- **IPv6 DSCP Service** — Specify the IP DiffServ Code Point (DSCP) value, which is defined as the high-order six bits of the Service Type octet in the IPv6 header. This is an optional configuration. Enter an integer from 0 to 63. The IPv6 DSCP can be selected from one of the DSCP keywords in the menu. To specify a DSCP by its numeric value, select the Other option in the menu, and a text box displays for entering the numeric value.

Configuring an IPv6 ACL Rule by Using the CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- ACL Commands

Downloaded from www.Manualslib.com manuals search engine

ACL Bind Configuration

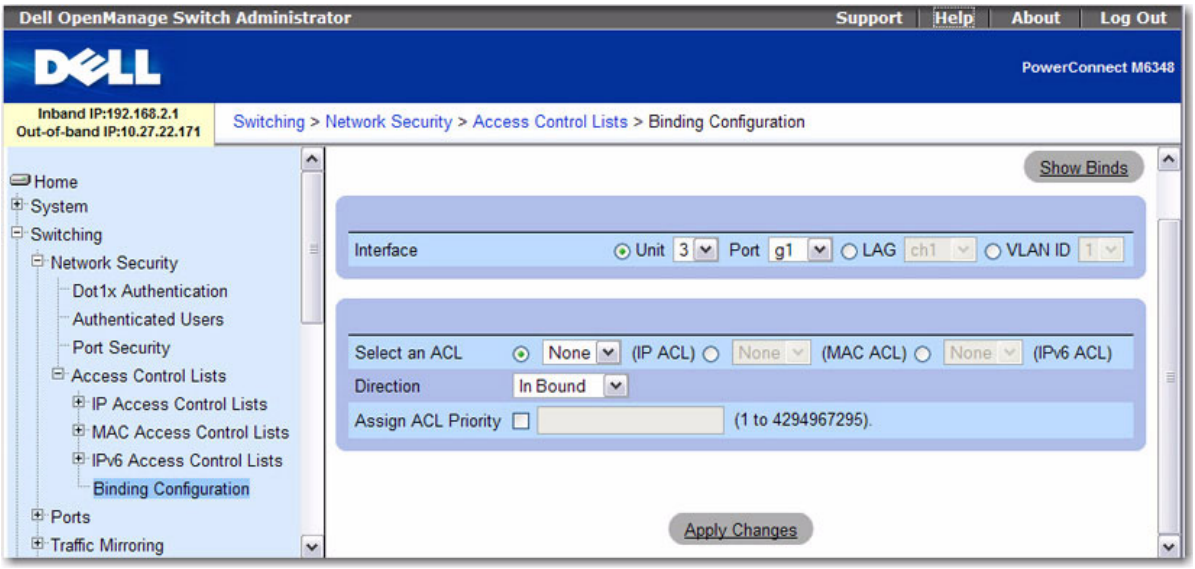
When an ACL is bound to an interface, all the rules that have been defined are applied to the selected interface. Use the **ACL Bind Configuration** page to assign ACL lists to ACL Priorities and Interfaces.

From the Web interface, you can configure the ACL rule in the ingress or egress direction so that the ACLs implement security rules for packets entering or exiting the port. You can apply ACLs to any physical (including 10 Gb) interface, LAG, or routing port.

NOTE: Binding an ACL in the egress direction is not supported by the PowerConnect M6220. IP ACLs may be bound to an Ethernet interface in the egress direction.

To display the **ACL Bind Configuration** page, click **Switching > Network Security > Access Control Lists > Binding Configuration** in the tree view.

Figure 7-18. ACL Bind Configuration



The **ACL Bind Configuration** page contains the following fields:

- **Interface** — Radio buttons permit selection of interface by Unit/port, LAG, or VLAN.
- **Select an ACL** — Selects the ACL type to which incoming packets are matched. Packets can be matched to IP-based, MAC-based, or IPv6-based ACLs. Valid combinations of ACLs that can be bound to any interface or VLAN are:

  IP and MAC ACLs can be bound together to an interface or VLAN but not to IPv6 ACLs.
- **Direction** — Specifies the packet filtering direction for ACL. Binding ACL for Interface and LAGs are:
  - IPv4 ACLs can be bound in both inbound and outbound.
  - MAC and IPv6 ACLs can be bound only in the inbound direction on the PowerConnect M6220.
  - VLANs — IPv4, MAC, and IPv6 ACLs can only be bound in the inbound direction on the PowerConnect M6220.

Downloaded from www.Manualslib.com manuals search engine

– **Assign ACL Priority** — Assigns the priority of this ACL. If more than one ACL is applied to an interface, then the match criteria for the highest priority ACLs are checked first.

Assigning an ACL to an Interface

1. Open the **ACL Bind Configuration** page.
2. In the **Interface** field, specify the Unit and Port, LAG, or VLAN to configure.
3. Select the IP, IPv6, or MAC ACL in the **Select an ACL** field.

   Note: Whenever an ACL is assigned on a port, LAG, or VLAN, flows from that ingress interface that do not match the ACL are matched to the default rule, which is Drop unmatched packets.
4. Specify the priority in **Assign ACL Priority**.
5. Click **Apply Changes**.

   The ACL is attached to the specified interface(s).

Removing an Interface from an ACL

1. Open the **ACL Bind Configuration** page.
2. Click **Show All**.
3. In the Interface field, specify the Unit and Port, LAG, or VLAN to view the ACL bindings for that interface.
4. Select the **Remove** check box for one or more ACLs to remove.
5. Click **Apply Changes**.

   The specified ACL(s) are removed from the interface.

Assigning ACL Membership Using the CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- ACL Commands

Downloaded from www.Manualslib.com manuals search engine

Configuring Ports

The **Ports** menu page provides links for configuring port functionality, including advanced features such as storm control and port mirroring, and for performing virtual port tests.

To display the page, click **Switching > Ports** in the tree view. The **Ports** menu page contains links to the following features:

- Global Parameters
- Port Configuration
- Protected Port Configuration
- LAG Configuration
- Storm Control

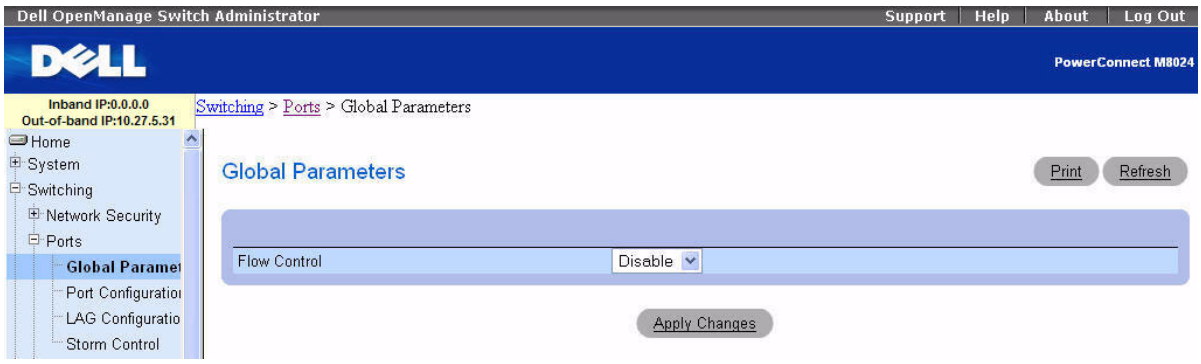
Global Parameters

Use the Global Parameters to configure Flow Control. Flow Control allows traffic from one switch to be throttled for a specified period of time, and is defined for switches that are directly connected. Flow Control can only be set for ports configured as full-duplex mode of operation. Since ports set to auto negotiate may not be added as LAG members, LAG member ports cannot have flow control configured to auto.

Note: Flow Control is incompatible with head of line blocking prevention mode. The switch can operate in either mode, but not at the same time.

To display the **Global Parameters** page, click **Switching > Ports > Global Parameters** in the tree view.

Figure 7-19. Global Port Parameters



The **Global Parameters** page contains the following field:

- **Flow Control** — Select enabled or disabled from the drop-down menu. This command affects all ports in the stack. The default value is enabled.
  - **Enable** — Turns on the ingress back pressure mechanism of the switch.
  - **Disable** — Restores the switch operation to head of line blocking prevention.

Downloaded from www.Manualslib.com manuals search engine

Enabling Ingress Backpressure

1. Open the **Ports Global Parameters** page.
2. Select Enable from the drop-down menu in the **Flow Control** field.
3. Click **Apply Changes**.
4. Ingress backpressure is now enabled.

Configuring Flow Control Using the CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- Ethernet Configuration Commands

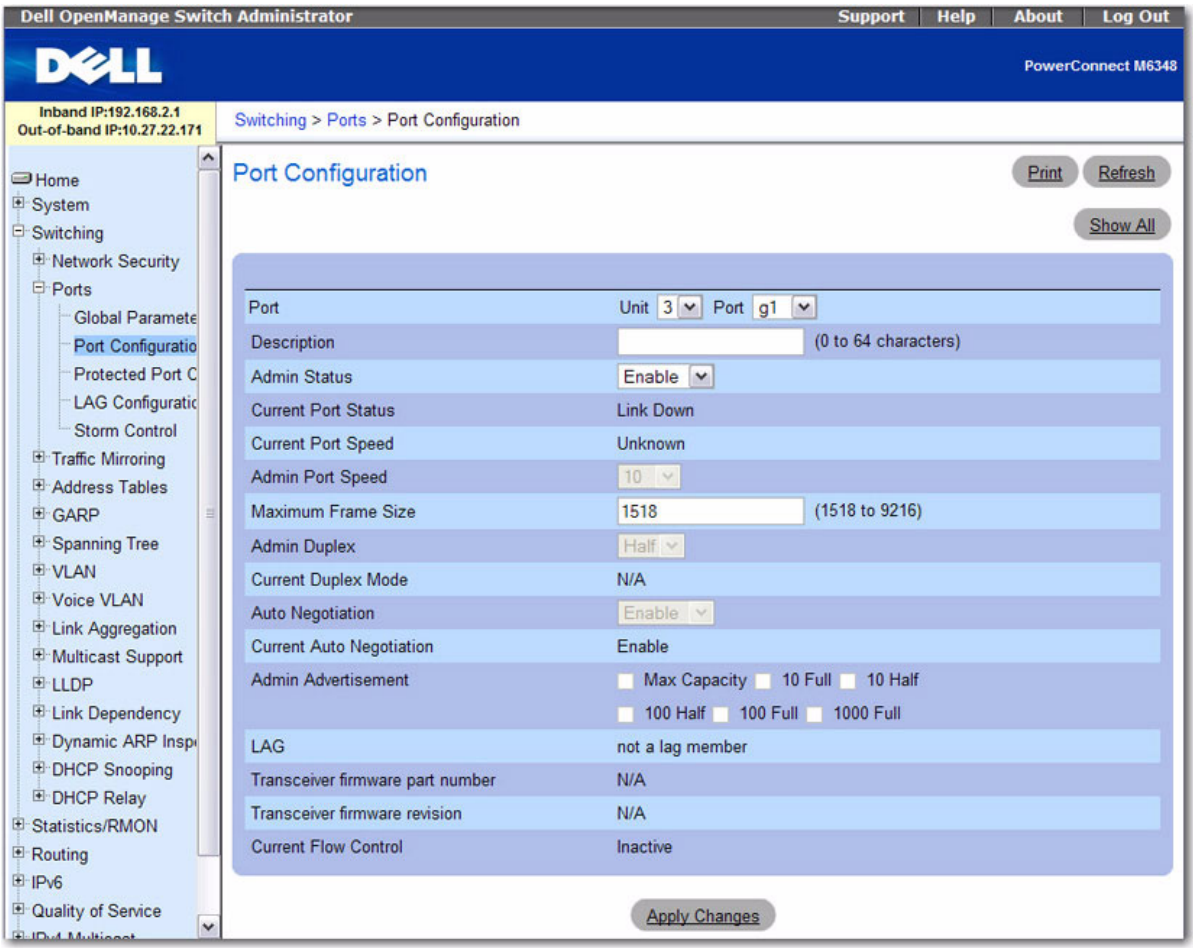
Port Configuration

Use the **Port Configuration** page to define port parameters.

To display the **Port Configuration** page, click **Switching > Ports > Port Configuration** in the tree view.

Downloaded from www.Manualslib.com manuals search engine

Figure 7-20. Port Configuration



The **Port Configuration** page contains the following fields:

- **Port** — Specifies the Unit and Port for which port parameters are defined.
- **Description (0–64 Characters)** — Provides a brief interface description, such as Ethernet.
- **Admin Status** — Enables (Up) or disables (Down) traffic forwarding through the port.
- **Current Port Status** — Specifies whether the port is currently operational or non-operational.
- **Current Port Speed** — Displays the actual synchronized port speed (bps).
- **Admin Port Speed** — Forces the port speed to the selected value (10M, 100M, or 10000M).For the PowerConnect M8024, the only available speed is 10000M.
- **Maximum Frame Size (1518–9216)**— Specifies the threshold beyond which packets exceeding this size are dropped. Default is 1518.
- **Admin Duplex** — Specifies the port duplex mode.

Downloaded from www.Manualslib.com manuals search engine

- **Full** — Indicates that the interface supports transmission between the switch and the client in both directions simultaneously.

- **Current Duplex Mode** — Displays the synchronized port duplex mode.
- **Auto Negotiation** — Enables Auto Negotiation on the port. Auto Negotiation is a protocol between two link partners that enables a port to advertise its transmission rate, duplex mode, and flow control abilities to its partner.
- **Current Auto Negotiation** — Displays the current Auto Negotiation setting.
- **Admin Advertisement** — Specifies the capabilities advertised by the port. The field values include:
- **LAG** — Displays LAG number if this port is a member of a LAG.
- **Current Flow Control** — Indicates the current Flow Control settings. Possible field values are:
  - **Active** — Flow Control is active.
  - **Inactive** — Flow Control is inactive.
- **Transceiver Firmware Version** — Displays firmware part number of port transceiver, if available. Valid only for SFX7101 transceivers on 10GBase-T non-stacking ports.
- **Image Firmware Version** — Displays the version of the image on the firmware.
- **Firmware Update Status** — Indicates the statue of the firmware on the switch:
  - **Up-to-date** — The firmware status is current.
  - **Outdated** — The firmware status is not current.
- **Max. Cable Length**— Displays the maximum cable length determined by current power backoff level.

Downloaded from www.Manualslib.com manuals search engine

Defining Port Parameters

1. Open the **Port Configuration** page.
2. Select a unit and port in the **Unit** and **Port** fields.
3. Define the available fields on the screen.
4. Click **Apply Changes**.

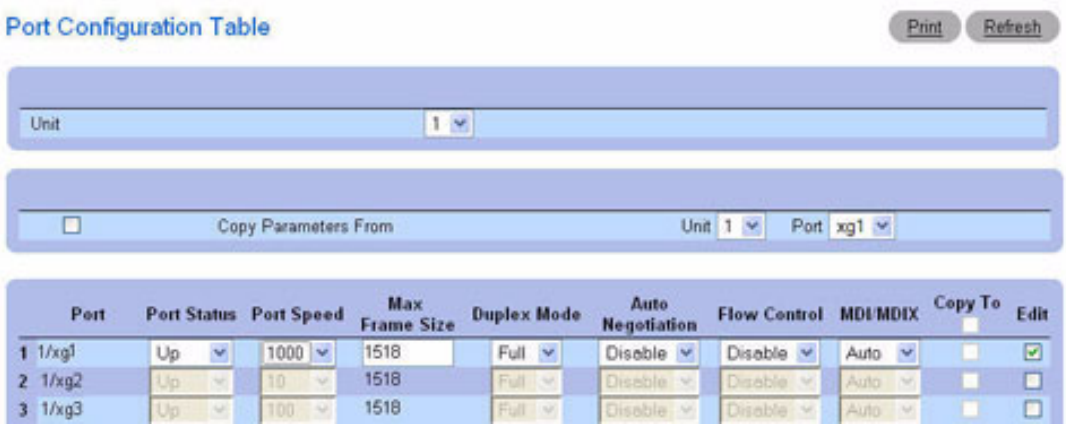
   The port parameters are saved to the switch.

Displaying the Port Table

1. Open the **Port Configuration** page.
2. Click **Show All**.

   The **Port Configuration Table** displays.

Figure 7-21. Port Configuration Table



3. Use the **Unit** drop-down menu to view the **Port Configuration Table** for other units in the stack, if they exist.

Copying Port Configuration Settings

1. Open the **Port Configuration** page.
2. Click **Show All**.

   The **Port Configuration Table** displays.
3. Specify the Unit and Port you are copying from in **Copy Parameters From**.
4. Click **Copy To** for each Port to receive these parameters.
5. Click **Apply Changes**.

   The Port Configuration settings are copied, and the device is updated.

Downloaded from www.Manualslib.com manuals search engine

Modifying Port Configuration Settings for Multiple Ports

1. Open the **Port Configuration** page.
2. Click **Show All**.

   The **Port Configuration Table** displays.
3. Click **Edit** for each Port to modify.
4. Edit the Port Configuration fields as needed.
5. Click **Apply Changes**.

   The Port Configuration settings are modified, and the device is updated.

Configuring Ports with CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

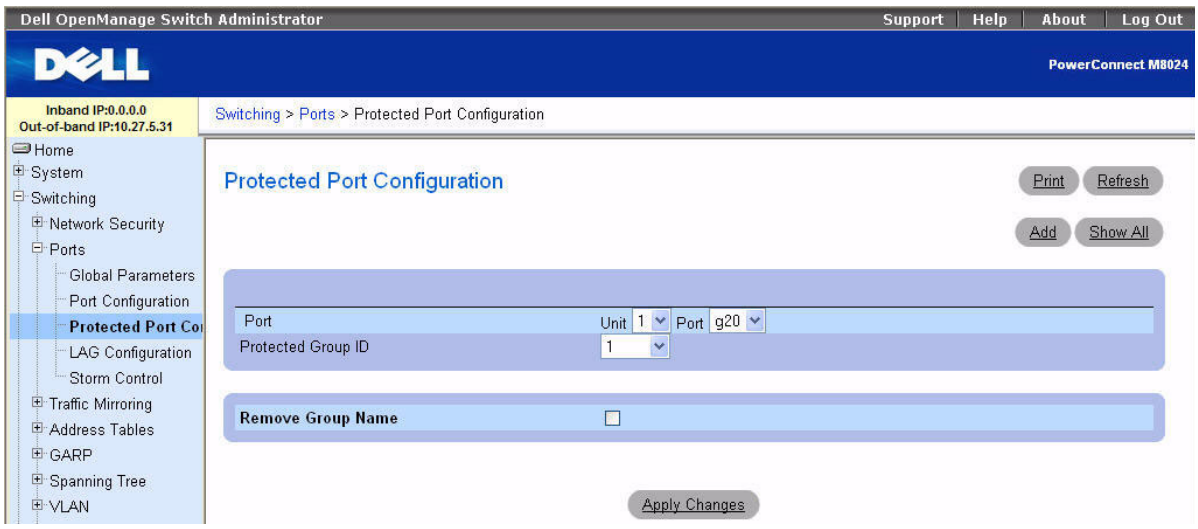
- Ethernet Configuration Commands

Protected Port Configuration

Use the **Protected Port Configuration** page to specify a Layer 2 security feature, Private VLAN Edge (PVE) ports, that provides port-based security between ports that are members of the same VLAN. Traffic from protected ports is sent only to the uplink ports and cannot be sent to other ports within the VLAN.

To display the **Port Configuration** page, click **Switching > Ports > Protected Port Configuration** in the tree view.

Figure 7-22. Protected Port Configuration



Downloaded from www.Manualslib.com manuals search engine

The **Protected Port Configuration** page contains the following fields:

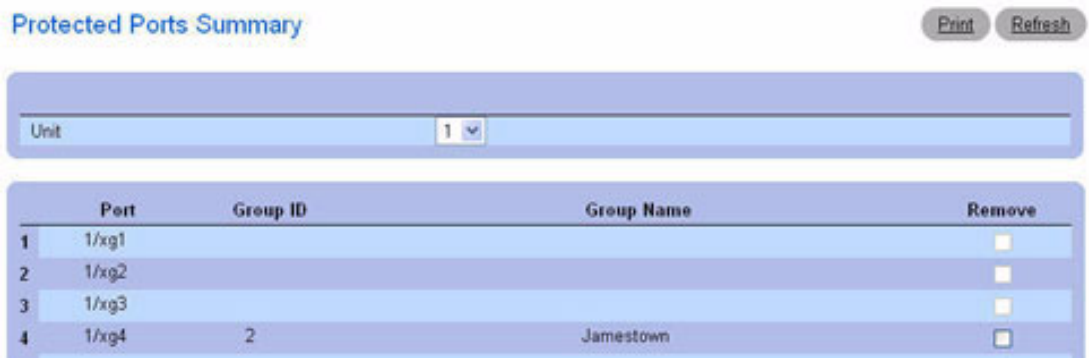
- **Port** — Specifies the Unit and Port for which port parameters are defined.
- **Protected Group ID** — Drop-down menu used to assign a port to Group 0, 1, or 2.
- **Remove Group Name** — Check this box to disassociate the selected port from the protected group.

Displaying the Protected Port Table

1. Open the **Protected Port Configuration** page.
2. Click **Show All**.

   The **Protected Ports Summary** table displays.

Figure 7-23. Protected Port Summary Table



3. Select the **Remove** check box and click **Apply Changes** to disassociate a port from a protected group.
4. Use the **Unit** drop-down menu to view the **Protected Port Summary** table for other units in the stack, if they exist.

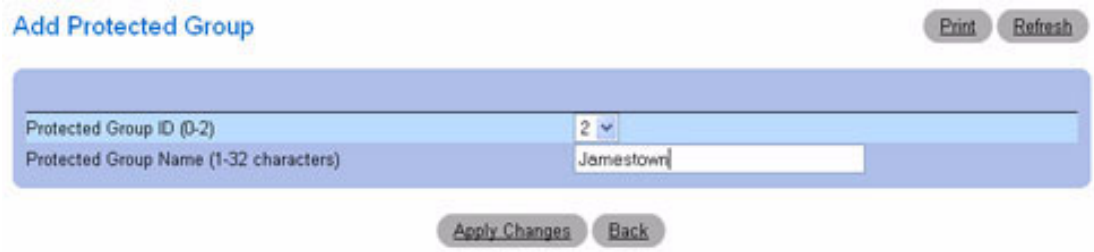
Adding Protected Port Groups

1. Open the **Protected Port Configuration** page.
2. Click **Add**.

   The **Add Protected Group** displays.

Downloaded from www.Manualslib.com manuals search engine

Figure 7-24. Add Protected Port



3. Use the drop-down menu to assign the numeric designation 0, 1, or 2 to the **Protected Group ID**.
4. Enter a **Protected Group Name (1–32 characters)**.
5. Click **Apply Changes**.

   The Protected Group settings are copied, and the device is updated.

Configuring Protected Ports With CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

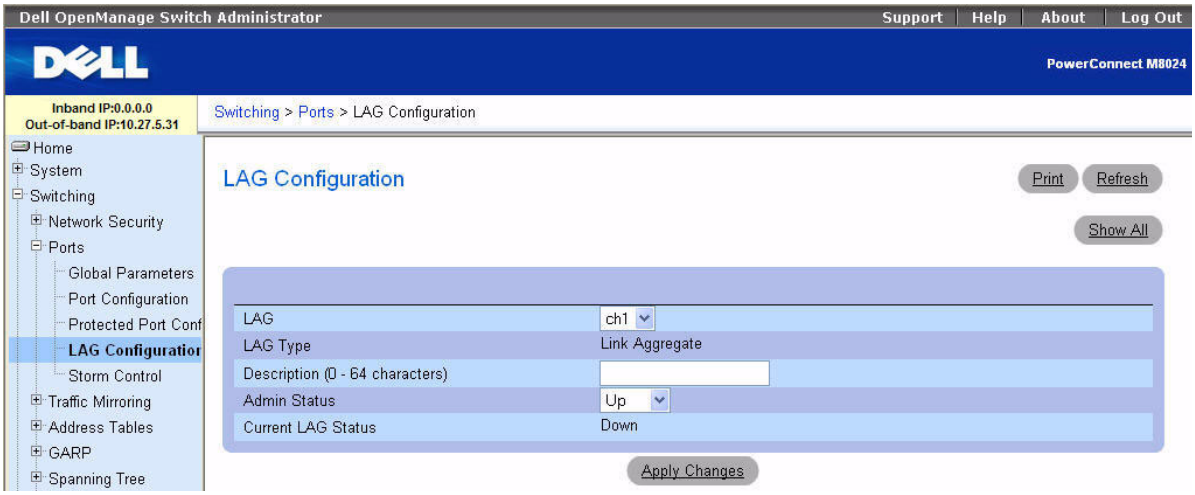
- Switchport Protected Commands

LAG Configuration

Link Aggregation allows one or more full duplex Ethernet links to be aggregated together to form a Link Aggregation Group (LAG). The switch can treat LAG as if it were a single link.

To display the **LAG Configuration** page, click **Switching > Ports > LAG Configuration** in the tree view.

Figure 7-25. LAG Configuration



The **LAG Configuration** page contains the following fields:

Downloaded from www.Manualslib.com manuals search engine

- **LAG** — Contains a list of LAG numbers.
- **LAG Type** — The port types that comprise the LAG.
- **Description (0–64 Characters)** — Description of the port.
- **Admin Status** — Enables or disables traffic forwarding through the selected LAG.
- **Current LAG Status** — Indicates whether the selected LAG is Up or Down.

Defining LAG Parameters

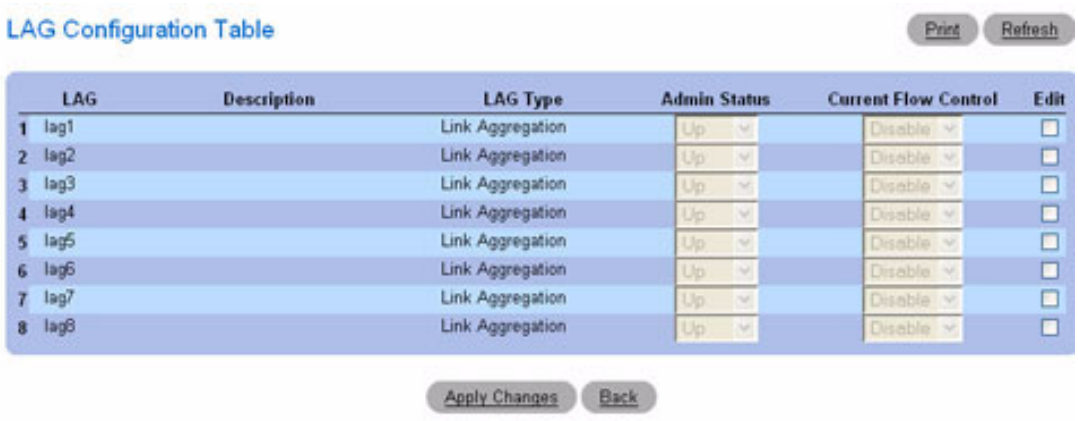
1. Open the **LAG Configuration** page.
2. Select a LAG in the **LAG** field.
3. Define the available fields on the screen.
4. Click **Apply Changes**.

   The LAG parameters are saved to the switch.

Displaying the LAG Configuration Table

1. Open the **LAG Configuration** page.
2. Click **Show All**.
3. The **LAG Configuration Table** displays.

Figure 7-26. LAG Configuration Table



Editing LAG Parameters

1. Open the **LAG Configuration** page.
2. Click **Show All**.
3. The **LAG Configuration Table** displays.
4. Check **Edit** for all LAGs to be modified.

Downloaded from www.Manualslib.com manuals search engine

5. **Admin Status** and **Description** can now be edited as needed.
6. Click **Apply Changes**.

   The LAG parameters are saved to the switch.

Configuring LAGs with CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- Port Channel Commands

Storm Control

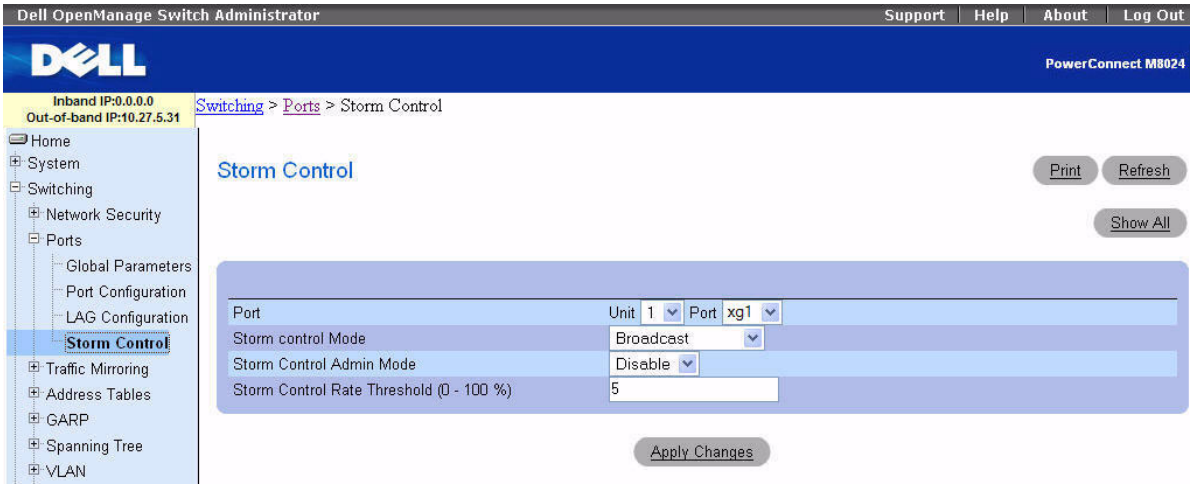
A broadcast storm is the result of an excessive number of broadcast messages simultaneously transmitted across a network by a single port. Forwarded message responses can overload network resources and/or cause the network to time out.

Your switch measures the incoming broadcast/multicast/unknown unicast packet rate per port and discards packets when the rate exceeds the defined value. Storm control is enabled per interface, by defining the packet type and the rate at which the packets are transmitted.

Use the **Storm Control** page to enable and configure storm control.

To display the **Storm Control** interface, click **Switching > Ports > Storm Control** in the tree view.

Figure 7-27. Storm Control



The **Storm Control** page contains the following fields:

- **Port** — Specifies the **Unit** and **Port** for which storm control is enabled.
- **Storm Control Mode** — Specifies the mode of broadcast affected by storm control.
  - **Broadcast** — If the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped.

Downloaded from www.Manualslib.com manuals search engine

– **Multicast** — If the rate of L2 multicast traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped.

– **Unknown Unicast** — If the rate of unknown L2 unicast (destination lookup failure) traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped.

- **Storm Control Admin Mode** — Enables or Disables Storm Control.
- **Storm Control Rate Threshold (0–100%)** — Specifies the maximum rate at which unknown packets are forwarded. The range is a percent of the total threshold.

Defining Storm Control Port Parameters

1. Open the **Storm Control** interface.
2. Edit the fields on the screen.
3. Click **Apply Changes**.

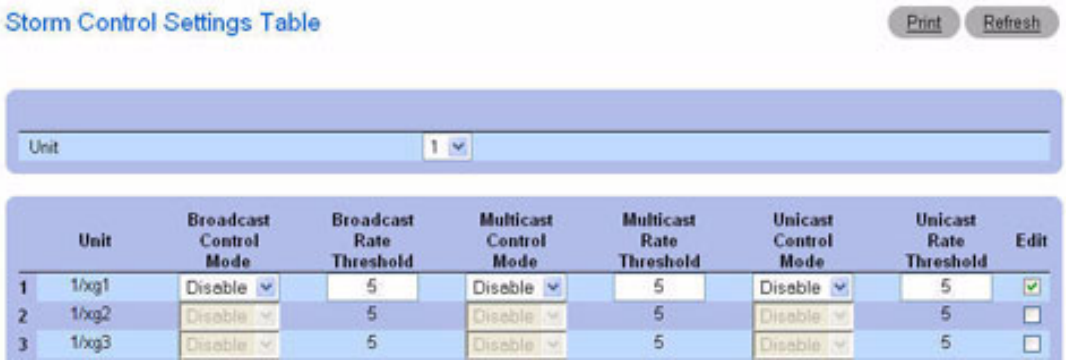
   The storm control port parameters are saved to the switch.

Displaying the Storm Control Settings Table

1. Open the **Storm Control** interface.
2. Click **Show All**.

   The **Storm Control Settings Table** displays.

Figure 7-28. Storm Control Settings Table



3. Use the **Unit** drop-down menu to view the **Storm Control Settings Table** for other units in the stack, if they exist.

Downloaded from www.Manualslib.com manuals search engine

Modifying Broadcast Control

1. Open the **Storm Control** interface.
2. Click **Show All**.

   The **Storm Control Settings Table** displays.
3. Check **Edit** for each port that **Broadcast Control** is to be modified.
4. Edit **Broadcast Control** as needed.
5. Click **Apply Changes**.

   The storm control port parameters are saved to the switch.

Configuring Storm Control with CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- Ethernet Configuration Commands

Configuring Traffic Mirroring

Traffic mirroring allows the user to configure the switch to send copies of packets on a port that is being mirrored to the mirroring port. The mirroring can be port-based or flow-based.

Use the **Traffic Mirroring** menu page to define port mirroring sessions and configure flow-based mirroring.

To display this page, click **Switching > Traffic Mirroring** in the tree view. The **Traffic Mirroring** menu page contains links to the following features:

- Port Mirroring
- Flow Based Mirroring

Port Mirroring

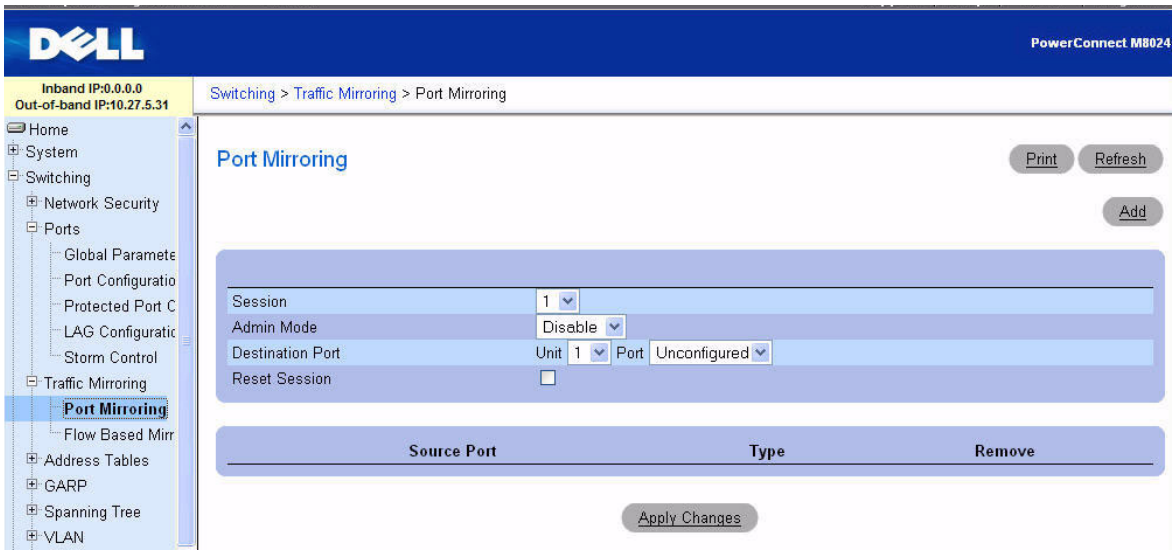
Port mirroring selects the network traffic for analysis by a network analyzer. This is done for specific ports of the switch. As such, many switch ports are configured as source ports and one switch port is configured as a destination port. You have the ability to configure how traffic is mirrored on a source port. Packets that are received on the source port, that are transmitted on a port, or are both received and transmitted, can be mirrored to the destination port.

The packet that is copied to the destination port is in the same format as the original packet on the wire. This means that if the mirror is copying a received packet, the copied packet is VLAN tagged or untagged as it was received on the source port. If the mirror is copying a transmitted packet, the copied packet is VLAN tagged or untagged as it is being transmitted on the source port.

To display the **Port Mirroring** page, click **Switching > Traffic Mirroring > Port Mirroring** in the tree view.

Downloaded from www.Manualslib.com manuals search engine

Figure 7-29. Port Mirroring



The **Port Mirroring** page contains the following fields:

- **Session** — Specifies the monitoring session.
- **Admin Mode** — Enables or Disables the port mirroring.
- **Destination Port** — Select the port to which port traffic may be copied.
- **Reset Session** — Allows you to reset the port monitoring session.
- **Source Port** — Lists the source ports that have been added from the Add Source Port page.
- **Type** — Shows the type traffic monitored on the source port.

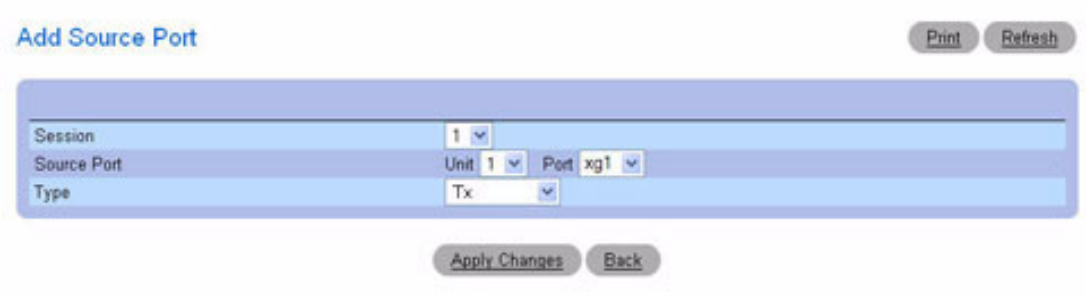
Adding a Port Mirroring Session

Note: A Port will be removed from a VLAN or LAG when it becomes a destination mirror.

1. Open the **Port Mirroring** page.
2. Click **Add** to display the **Add Source Port** page.

Downloaded from www.Manualslib.com manuals search engine

Figure 7-30. Add Source Port



3. Configure the following fields:

   Session — Select the session to monitor.

   Source Port —Select the unit and port from which traffic is mirrored. Up to four source ports can be mirrored to a destination port.

   Type — Specifies the type of traffic monitored. Possible field values are:

   TX — Monitors transmitted packets only.

   RX — Monitors received packets only.

   TX and RX — Monitors transmitted and received packets.

4. Click **Apply Changes**.

   The new port mirroring session is enabled for the unit and port, and the device is updated. The source port appears in the Source Port table on the Port Mirroring page.

Modifying a Port Mirroring Session

1. Open the **Port Mirroring** page.
2. Modify the fields.
3. Click **Apply Changes**.

   The port mirroring session fields are modified, and the device is updated.

Removing a Port Mirroring Session

1. Open the **Port Mirroring** page.
2. Select the **Reset Session** check box.
3. Click **Apply Changes**.

   The port mirroring session is removed, and the device is updated.

Downloaded from www.Manualslib.com manuals search engine

Configuring a Port Mirroring Session Using CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- Port Monitor Commands

Flow Based Mirroring

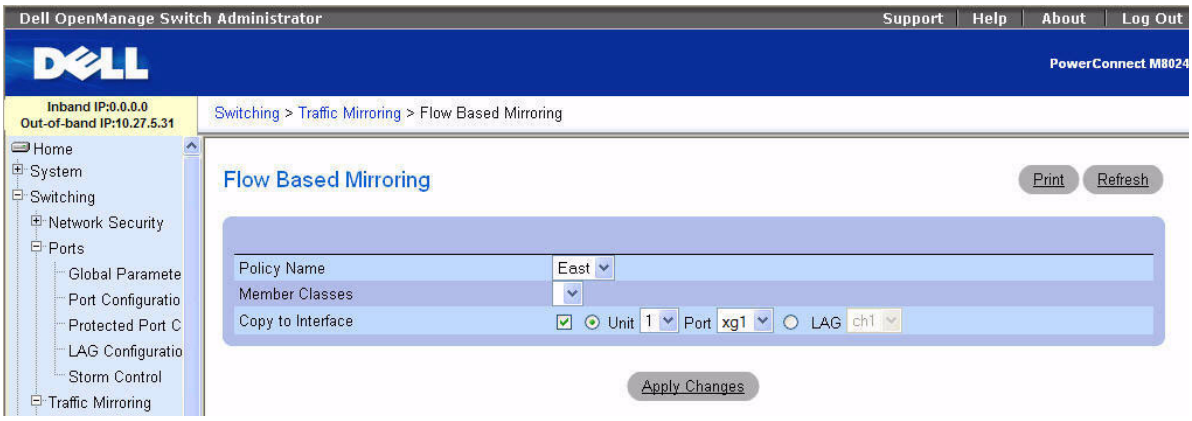
The flow based mirroring feature builds upon the DiffServ component in QoS. In QoS, the user creates traffic classes to define match criteria, then policies to define the action to be taken on that traffic class.

Flow based mirroring allows the user to copy certain types of traffic to a single destination port. This provides flexibility—instead of mirroring all ingress or egress traffic on a port, the switch can mirror a subset of that traffic. You can configure the switch to mirror flows based on Layer 2, Layer 3, and Layer 4 information.

Use the **Flow Based Mirroring** page to specify flow-based mirroring ports.

To display the **Flow Based Mirroring** page, click **Switching > Traffic Mirroring > Flow Based Mirroring** in the tree view.

Figure 7-31. Flow Based Mirroring



The **Flow Based Mirroring** page contains the following fields:

- **Policy Name** — Selects policy to associate with a traffic class. Policy Name is defined using the DiffServ "Policy Configuration" web page.
- **Member Classes** — Selects the traffic class associated with this policy. Member Class is defined using the DiffServ "Class Configuration" web page.
- **Copy to Interface** — When checked, this feature permits packets to be copied to either a unit/port or LAG.

Downloaded from www.Manualslib.com manuals search engine

Copying Mirroring to a Destination Port

1. Open the **Flow Based Mirroring** page.
2. Specify **Policy Name** and **Member Class**, and select the destination unit and port to be affected in **Copy to Interface**.
3. Click **Apply Changes**.

   The flow-based mirroring details are copied to the specified port, and the device is updated.

Configuring Flow-based Mirroring Using CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- QOS Commands

Configuring Address Tables

MAC addresses are stored in either the static or dynamic address table. Static addresses are defined by you. Dynamic addresses are learned by the system, and are erased after a time-out. A packet addressed to a destination stored in one of the tables is forwarded immediately to the ports. The static and dynamic address tables can be sorted by Interface, VLAN ID, or VLAN Name. In addition, addresses can be added to the static and dynamic address tables.

To display the **Address Tables** menu page, click **Switching > Address Tables** in the tree view. The **Address Tables** menu page contains links to the following features:

- Static Address Table
- Dynamic Address Table

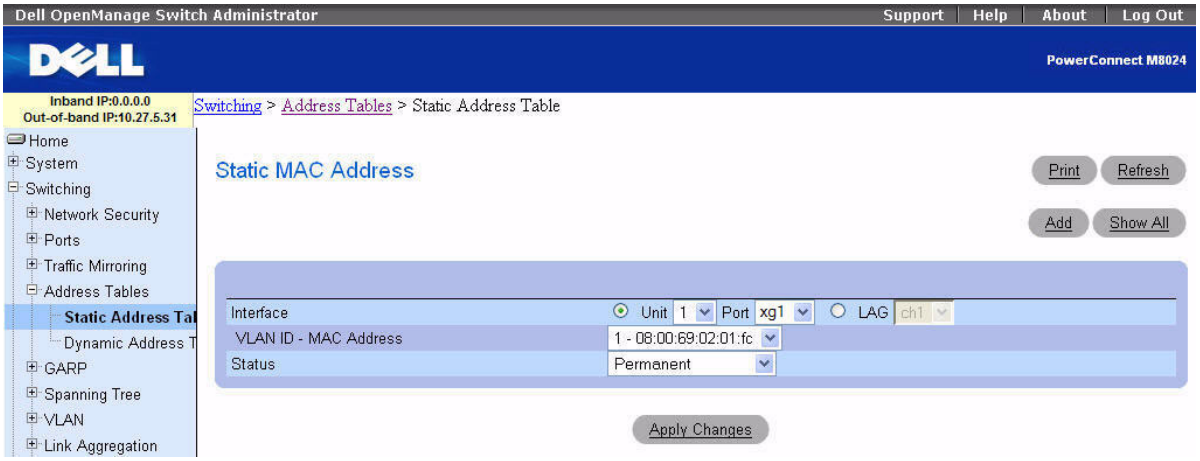
Static Address Table

The **Static MAC Address** page contains a list of static MAC addresses. A static address can be added and removed from the Static MAC Address Table.

To display the **Static MAC Address** page, click **Switching > Address Tables > Static Address Table** in the tree view.

Downloaded from www.Manualslib.com manuals search engine

Figure 7-32. Static MAC Address



The **Static MAC Address** page contains the following fields:

- **Interface** — Specifies the Unit and Port or LAG to which the static MAC address is applied. To view addresses for a different Unit/Port or LAG, change the Interface listed here.
- **VLAN ID - MAC Address** — Specifies VLAN ID attached to the MAC Address and the MAC address(es) included in the current static address list.

Note: Only MAC addresses assigned to the specified interface and VLAN are displayed.

- **Status** — Specifies status of the MAC address. Possible values are:
  - **Permanent** — The MAC address is permanent.
  - **Secure** — Guarantees that a locked port MAC address is not deleted.
  - **Delete on Reset** — The MAC address is deleted when the switch is reset.
  - **Delete on Timeout** — The MAC address is deleted when a timeout occurs.

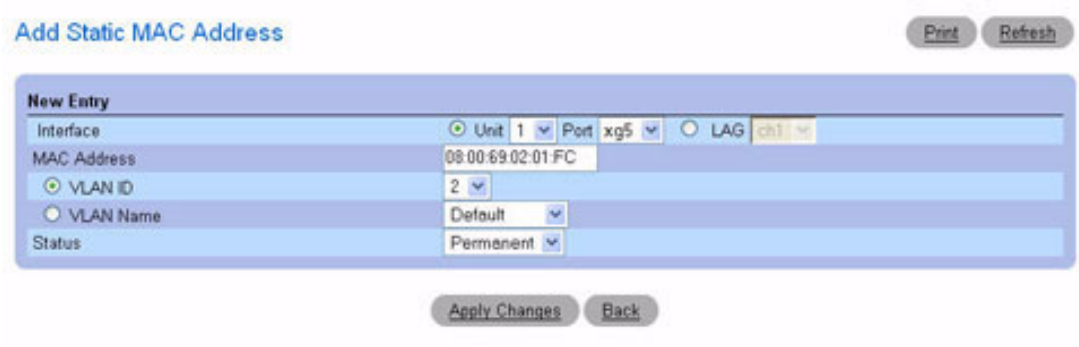
Adding a Static MAC Address

1. Open the **Static MAC Address** page.
2. Click **Add**.

   The **Add Static MAC Address** page displays.

Downloaded from www.Manualslib.com manuals search engine

Figure 7-33. Adding Static MAC Address



3. Complete the fields as needed.
4. Click **Apply Changes**.

   The new static address is added to the **Static MAC Address Table**, and the device is updated.

Modifying a Static Address in the Static MAC Address Table

1. Open the **Static MAC Address** page.
2. Modify the fields.
3. Click **Apply Changes**.

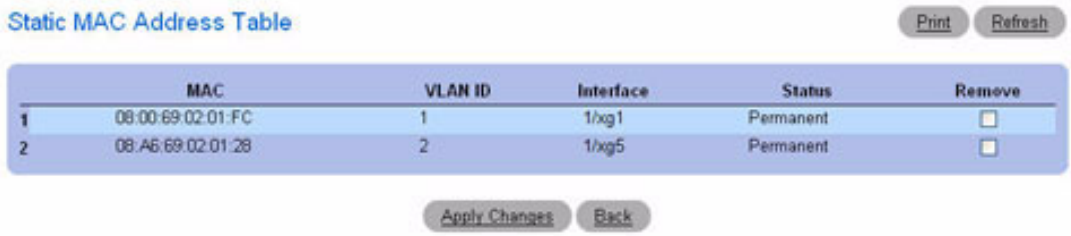
   The static MAC address is modified, and the device is updated.

Displaying the Static MAC Address Table

1. Open the **Static MAC Address** page.
2. Click **Show All**.

   The **Static MAC Address Table** displays all existing static MAC addresses.

Figure 7-34. Static MAC Address Table



Downloaded from www.Manualslib.com manuals search engine

Removing a Static Address from the Static Address Table

1. Open the **Static MAC Address** page.
2. Click **Show All** to display the **Static MAC Address Table**.
3. Check the **Remove** check box for the address to be removed.
4. Click **Apply Changes**.

   The static address is deleted, and the device is updated.

Configuring Static Address Parameters Using CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- Address Table Commands

Dynamic Address Table

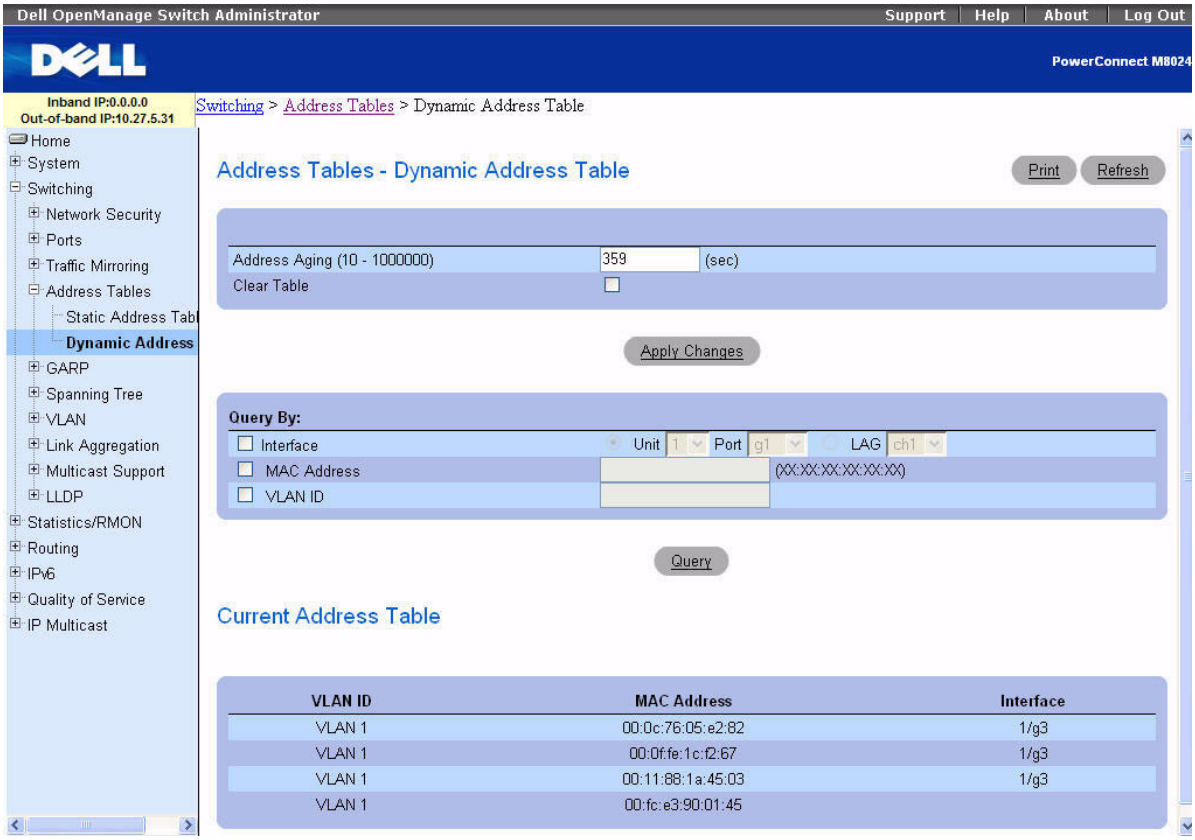
The **Dynamic Address Table** page contains fields for querying information in the dynamic address table, including the interface type, MAC addresses, VLAN, and table sorting key. Packets forwarded to an address stored in the address table are forwarded directly to those ports.

The **Dynamic Address Table** also contains information about the aging time before a dynamic MAC address is removed from the table.

To display the **Dynamic Address Table**, click **Switching > Address Tables > Dynamic Address Table** in the tree view.

Downloaded from www.Manualslib.com manuals search engine

Figure 7-35. Dynamic Address Table



The **Dynamic Address Table** contains the following fields:

- **Address Aging (10–1000000)** — Specifies aging time in seconds before a dynamic MAC address is erased. The default value is 300 seconds.
- **Clear Table** — Clears all dynamic MAC address data from the table when checked and **Apply Changes** is clicked.
- **The** Dynamic Address Table **can be queried by:**
  - **Interface** — Specifies Unit and Port queried for an address.
  - **LAG** — Specifies the LAG queried for an address.
  - **MAC Address** — Specifies the MAC address queried for an address.
  - **VLAN ID** — Specifies the VLAN number (to which the MAC address is attached) that is queried for an address.
- The **Current Address Table** contains dynamic address parameters by which packets are directly forwarded to the ports. The **Current Address Table** contains the following fields:
- **VLAN ID** — Displays the VLAN Tag value.
- **MAC Address**— Displays the MAC address.

Downloaded from www.Manualslib.com manuals search engine

- **Interface** — Displays the port number.

Defining the Aging Time

1. Open the **Dynamic Address Table** page.
2. Define the **Address Aging** field.
3. Click **Apply Changes**.

   The aging time is modified, and the device is updated.

Querying the Dynamic Address Table

1. Open the **Dynamic Address Table** page.
2. Define the parameter by which to query the **Dynamic Address Table**.

   Entries can be queried by **Interface**, **LAG**, **MAC Address**, or **VLAN ID**.
3. Click **Query** to query the Dynamic Address Table.

Removing Data From the Dynamic Address Table

1. Open the **Dynamic Address Table** page.
2. Check **Clear Table**.
3. Click **Apply Changes**.

   The Dynamic Address Table is cleared of all data.

Querying and Sorting Dynamic Addresses Using CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- Address Table Commands

Configuring GARP

Generic Attribute Registration Protocol (GARP) is a general-purpose protocol that registers any network connectivity or membership-style information. GARP defines a set of switches interested in a given network attribute, such as VLAN or multicast address. The **GARP Timers** page is accessible from the **GARP** menu page.

To display the **GARP** menu page, click **Switching > GARP** in the tree view.

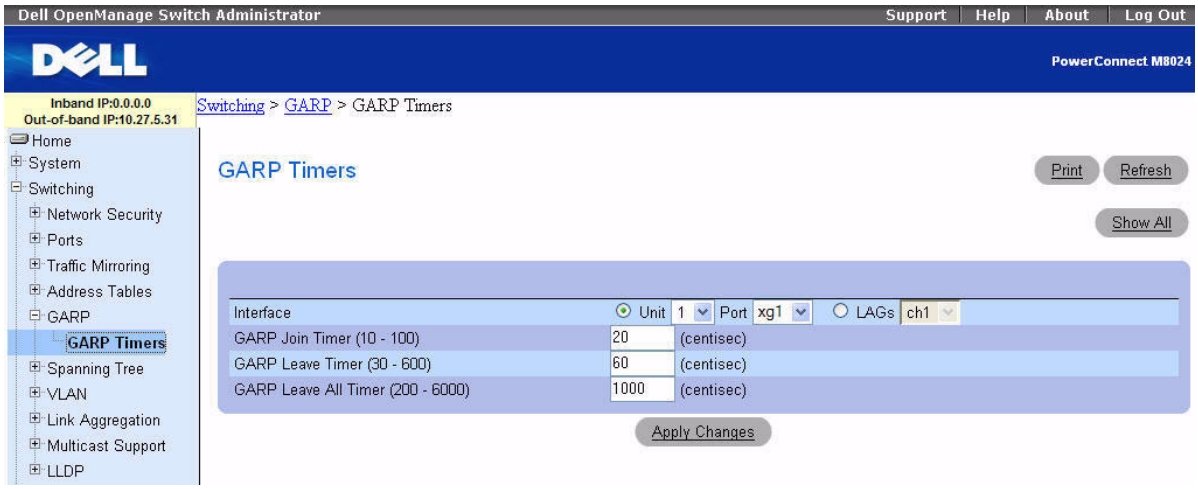
GARP Timers

The **GARP Timers** page contains fields for enabling GARP on the switch.

To display the **GARP Timers** page, click **Switching > GARP > GARP Timers** in the tree view.

Downloaded from www.Manualslib.com manuals search engine

Figure 7-36. GARP Timers



The **GARP Timers** page contains the following fields:

- **Interface** — Specifies the Unit and Port or LAG on which the GARP timer is enabled.
- **GARP Join Timer (10–100)** — Displays time, in centiseconds, that PDUs are transmitted. The possible field value is 10-100. The default value is 100 centisecs.
- **GARP Leave Timer (30–600)** — Displays time lapse, in centiseconds, that the switch waits before leaving its GARP state. Leave time is activated by a Leave All Time message sent/received, and cancelled by the Join message received. Leave time must be greater than or equal to three times the join time. The possible field value is 30–600. The default value is 60 centisecs.
- **GARP Leave All Timer (200–6000)** — Displays time lapse, in centiseconds, that all switches wait before leaving the GARP state. The leave all time must be greater than the leave time. The possible field value is 200–6000. The default value is 1000 centisecs.

Defining GARP Timers

1. Open the **GARP Timers** page.
2. Complete the fields.
3. Click **Apply Changes**.

   The parameters are copied to the selected ports or LAGs in the GARP Timers Table, and the device is updated.

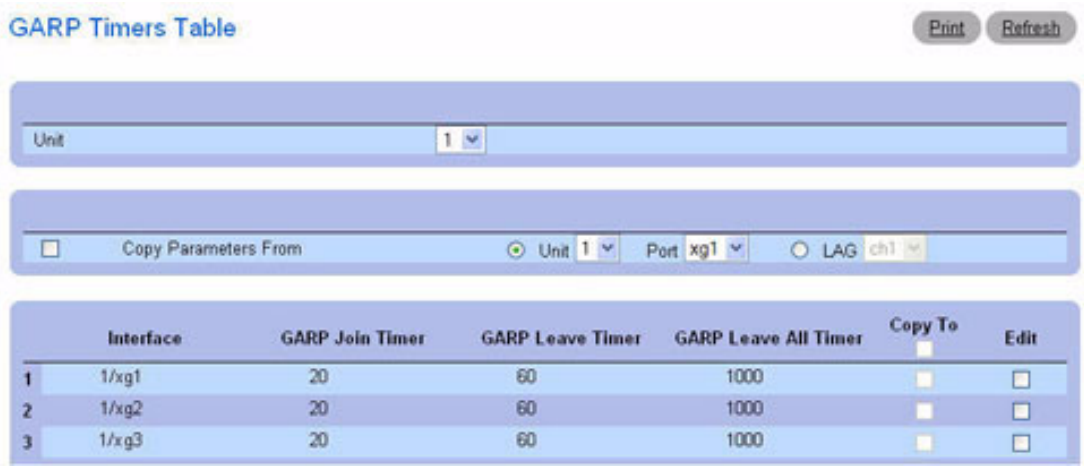
Displaying Parameters in the GARP Timers Table

1. Open the **GARP Timers** page.
2. Click **Show All**.

   The **GARP Timers Table** displays.

Downloaded from www.Manualslib.com manuals search engine

Figure 7-37. GARP Timers Table



3. Use the **Unit** drop-down menu to view the **GARP Timers Table** for other units in the stack, if they exist.

Copying GARP Timers Settings

1. Open the **GARP Timers** page.
2. Click **Show All**.

   The **GARP Timers Table** displays.
3. Specify the Unit and Port you are copying from in **Copy Parameters From**.
4. Click **Copy To** for each Interface to receive these parameters.
5. Click **Apply Changes**.

   The GARP Timers settings are copied, and the device is updated.

Modifying GARP Timers Settings for Multiple Ports

1. Open the **GARP Timers** page.
2. Click **Show All**.

   The **GARP Timers Table** displays.
3. Click **Edit** for each Interface to modify.
4. Edit the GARP Timers fields as needed.
5. Click **Apply Changes**.

   The GARP Timers settings are modified, and the device is updated.

Downloaded from www.Manualslib.com manuals search engine

Defining GARP Timers Using CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- GVRP Commands

Configuring the Spanning Tree Protocol

The Spanning Tree Protocol (STP) provides a tree topology for any arrangement of bridges. STP also provides one path between end stations on a network, eliminating loops. Spanning tree versions supported include Classic STP, Multiple STP, and Rapid STP.

Classic STP provides a single path between end stations, avoiding and eliminating loops. For information on configuring Classic STP, see "STP Global Settings."

Multiple Spanning Tree Protocol (MSTP) supports multiple instances of Spanning Tree to efficiently channel VLAN traffic over different interfaces. Each instance of the Spanning Tree behaves in the manner specified in IEEE 802.1w, Rapid Spanning Tree (RSTP), with slight modifications in the working but not the end effect (chief among the effects, is the rapid transitioning of the port to 'Forwarding'). The difference between the RSTP and the traditional STP (IEEE 802.1d) is the ability to configure and recognize full duplex connectivity and ports which are connected to end stations, resulting in rapid transitioning of the port to 'Forwarding' state and the suppression of Topology Change Notification. These features are represented by the parameters 'pointtopoint' and 'edgeport'. MSTP is compatible to both RSTP and STP. It behaves appropriately to STP and RSTP bridges. A MSTP bridge can be configured to behave entirely as a RSTP bridge or a STP bridge.

To display the **Spanning Tree** menu page, click **Switching > Spanning Tree** in the tree view. This **Spanning Tree** page contains links to the following STP procedures:

- STP Global Settings
- STP Port Settings
- STP LAG Settings
- Rapid Spanning Tree
- MSTP Settings
- MSTP Interface Settings

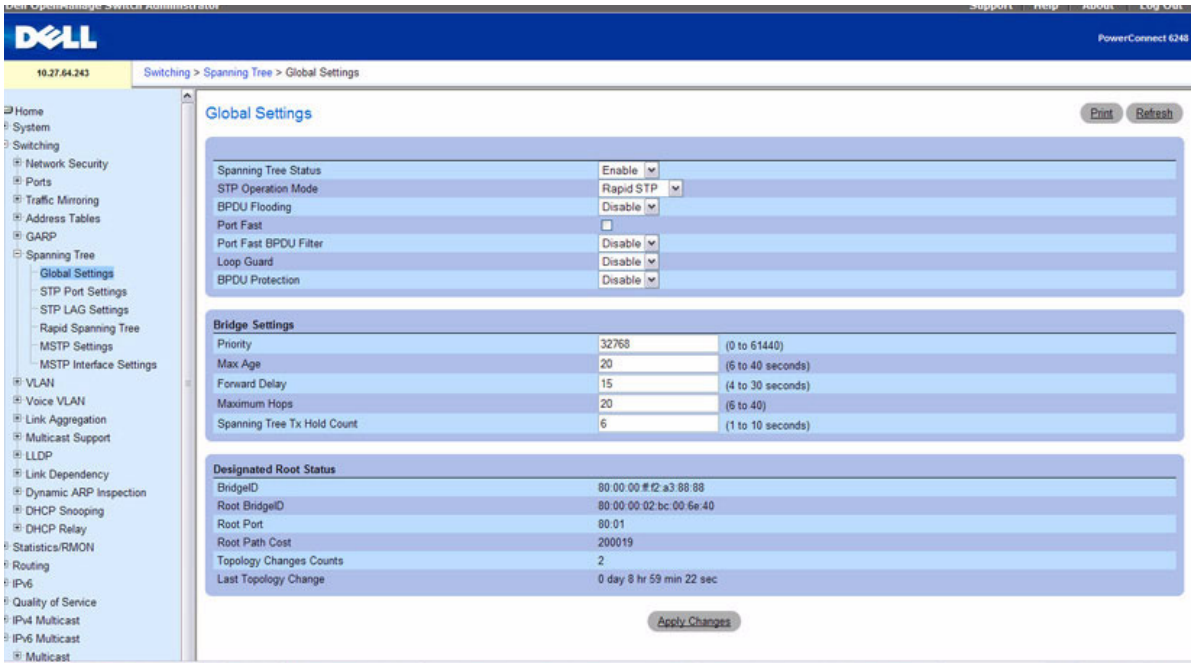
STP Global Settings

The **STP Global Settings** page contains fields for enabling STP on the switch.

To display the **STP Global Settings** page, click **Switching > Spanning Tree > Global Settings** in the tree view.

Downloaded from www.Manualslib.com manuals search engine

Figure 7-38. Spanning Tree Global Settings



The **STP Global Settings** page contains the following fields:

- **Spanning Tree Status** — Enables or disables RSTP, STP, or MSTP on the switch.
- **STP Operation Mode** — Specifies the STP mode by which STP is enabled on the switch. Possible field values are: **Classic STP, Rapid STP, and Multiple STP**.
- **BPDU Flooding** — Specifies Bridge Protocol Data Unit (BPDU) packet handling when the spanning tree is disabled on an interface. The possible field values are **Enable** or **Disable**. The default value is **Disable**.
- **Port Fast** — Enables Port Fast mode for all ports on the switch when checked. If Port Fast mode is enabled for a port, the Port State is automatically placed in the Forwarding state when the port link is up. Port Fast mode optimizes the time it takes for the STP protocol to converge. STP convergence can take 30-60 seconds in large networks.
- **Port Fast BPDU Filter** — Specifies BPDU Filter Mode on all ports which are enabled for Port Fast Mode. Possible values are **Enable** and **Disable**. The default value is **Disable**.
- **Loop Guard** — **Enables** or **disables** Loop Guard on all the ports.
- **BPDU Protection —** Disables a port in case a new switch tries to enter the already existing topology of STP. This keeps switches not originally part of an STP from influencing the STP topology.

  If set to Enable, when a BPDU is received on an edge port, that port is disabled. Once the port has been disabled it requires manual-intervention to be re-enabled.

Downloaded from www.Manualslib.com manuals search engine

Bridge Settings

- **Priority** — Specifies the bridge priority value. When switches or bridges are running STP, each are assigned a priority. After exchanging BPDUs, the switch with the lowest priority value becomes the root bridge. Valid values are from 0–61440. The default value is 32768.
- **Max Age** — Specifies the switch maximum age time, which indicates the amount of time in seconds a bridge waits before implementing a topological change. Valid values are from 6 to 40 seconds. The default value is 20 seconds.
- **Forward Delay** — Specifies the switch forward delay time, which indicates the amount of time in seconds a bridge remains in a listening and learning state before forwarding packets. Valid values are from 4 to 30 seconds.The default value is 15 seconds.
- **Maximum Hops** — Configure the maximum number of hops for the spanning tree. Valid values are from 6 to 40. The default value is 20.
- **Spanning Tree Tx Hold Count** — Configure the Bridge Tx Hold Count parameter for the spanning tree. Valid values are from 1 to 10 seconds. The default value is 6 seconds.

Designated Root Status

- **Bridge ID** — Displays the bridge ID.
- **Root Bridge ID** — Specifies the root bridge ID.
- **Root Port** — Displays port number that offers the lowest-cost path from this bridge to the root bridge. It is significant when the bridge is not the root. The default is zero.
- **Root Path Cost** — Displays the cost of the path from this bridge to the root.
- **Topology Changes Counts** — Displays the total amount of STP state changes that have occurred.
- **Last Topology Change** — Displays the total amount of time since the last topographic change. The time is displayed in day/hour/minute/second format, for example, 5 hours 10 minutes and 4 seconds.

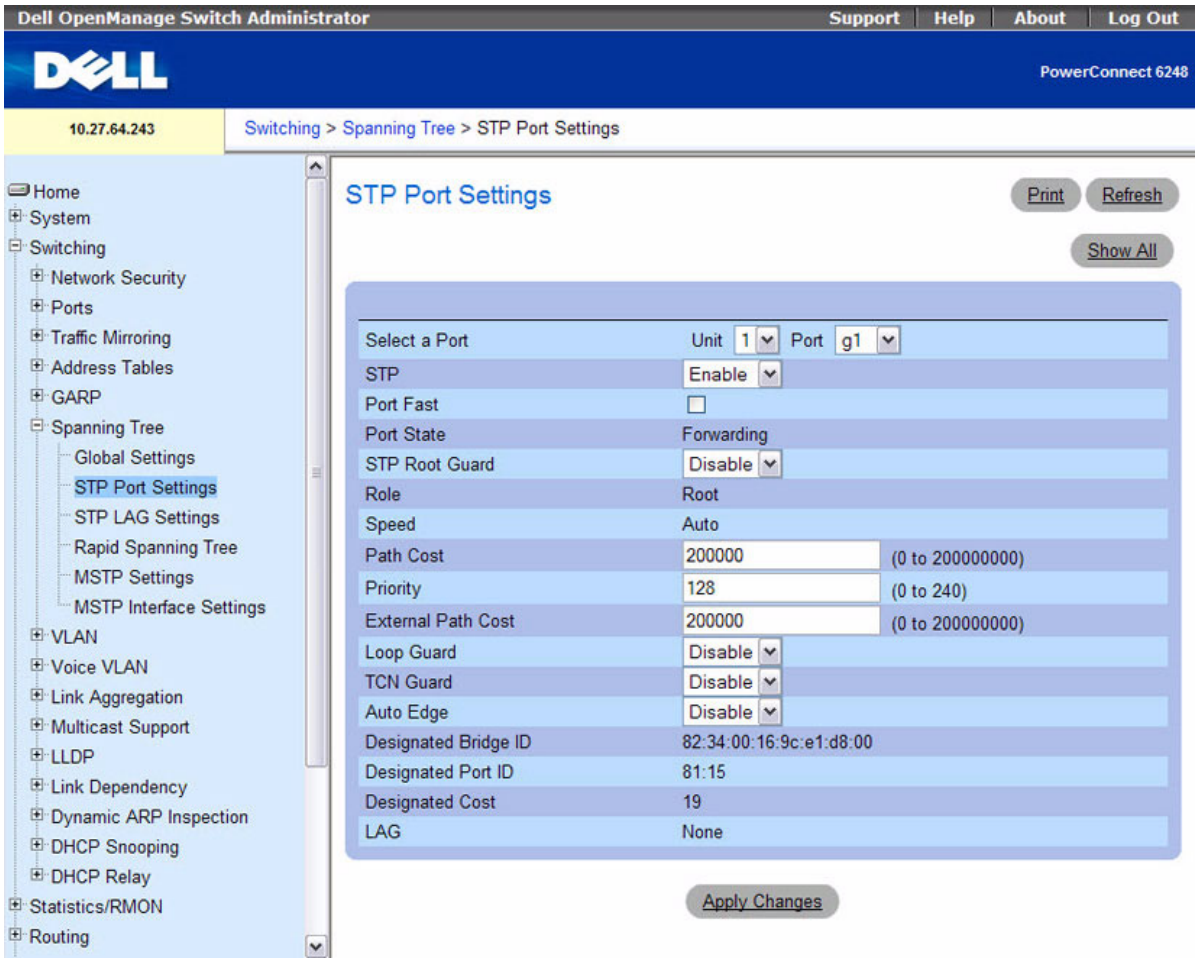
STP Port Settings

Use the **STP Port Settings** page to assign STP properties to individual ports.

To display the **STP Port Settings** page, click **Switching > Spanning Tree > STP Port Settings** in the tree view.

Downloaded from www.Manualslib.com manuals search engine

Figure 7-39. STP Port Settings



The **STP Port Settings** page contains the following fields:

- **Select a Port** — Specifies the Unit and Port on which STP is enabled.
- **STP** — Enables or disables STP on the port.
- **Port Fast** — Enables Port Fast mode for the port when checked. If Port Fast mode is enabled for a port, the **Port State** is automatically placed in the **Forwarding** state when the port link is up. STP convergence can take 30–60 seconds in large networks.
- **Port State**—Indicates the current STP state of a port. If enabled, the port state determines what forwarding action is taken on traffic. Possible port states are:
  - **Disabled** — STP is currently disabled on the port. The port forwards traffic while learning MAC addresses.

Downloaded from www.Manualslib.com manuals search engine

- **Blocking** — The port is currently blocked and cannot be used to forward traffic or learn MAC addresses.
- **Listening** — The port is currently in the listening mode. The port cannot forward traffic nor can it learn MAC addresses.
- **Learning** — The port is currently in the learning mode. The port cannot forward traffic, however, it can learn new MAC addresses.
- **Forwarding** — The port is currently in the forwarding mode. The port can forward traffic and learn new MAC addresses.

- **STP Root Guard** — Prevents the root of a Spanning Tree instance from changing unexpectedly. When a root bridge has root guard enabled and a superior BPDU arrives, that port is moved to a root-inconsistent state, which equates to the listening state. The root bridge is enforced.
- **Role** — Displays the role this port has in the STP topology. The port role will be one of the following values: Root Port, Designated Port, Alternate Port, Backup Port, Master Port or Disabled Port.
- **Speed** — Displays speed at which the port is operating.
- **Path Cost** — Specifies the port contribution to the root path cost. The path cost is adjusted to a higher or lower value, and is used to forward traffic when a path is being rerouted. A value of zero means the path cost is set according to the port's speed. The possible values are 0 to 200000000. The default value is 0.
- **Priority** — Specifies priority value of the port. The priority value influences the port choice when a bridge has two ports connected in a loop. The possible values are 0 to 240. The default value is 128.
- **External Path Cost** — Specifies the External Path Cost to a new value for the specified port in the spanning tree. Enter 0 to set the external path cost value automatically on the basis of Link Speed. The possible values are 0 to 200000000. The default value is 0.
- **Loop Guard** — Prevents a port from erroneously transitioning from blocking state to forwarding when the port stops receiving BPDUs. The port is marked as being in loop-inconsistent state. In this state, the port does not forward packets. The possible values are **Enable** or **Disable**.
- **TCN Guard** — Enabling the TCN Guard feature restricts the port from propagating any topology change information received through that port. This means that even if a port receives a BPDU with the topology change flag set to true, the port will not flush its MAC address table and send out a BPDU with a topology change flag set to true.
- **Auto Edge** — Enabling the Auto Edge feature allows the port to become an edge port if it does not see BPDUs for some duration.
- **Designated Bridge ID** — Displays the ID of the designated bridge.
- **Designated Port ID**— Displays the ID of the selected port.
- **Designated Cost** — Displays cost of the port participating in the STP topology. Ports with a lower cost are less likely to be blocked if STP detects loops.
- **LAG** — Displays LAG to which the port is attached.

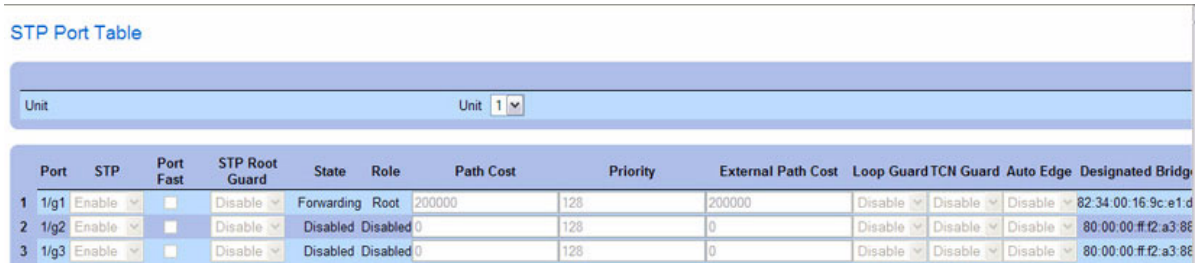
Downloaded from www.Manualslib.com manuals search engine

Displaying the STP Port Table and Configuring STP Port Settings

1. Open the **STP Port Settings** page.
2. Click **Show All**.

   The **STP Port Table** displays.

Figure 7-40. STP Port Table



3. Use the **Unit** drop-down menu to view the **STP Port Table** for other units in the stack, if they exist.
4. To change the STP settings for one or more ports, select the Edit option for the port(s), configure the desired settings, and then click **Apply Changes**.

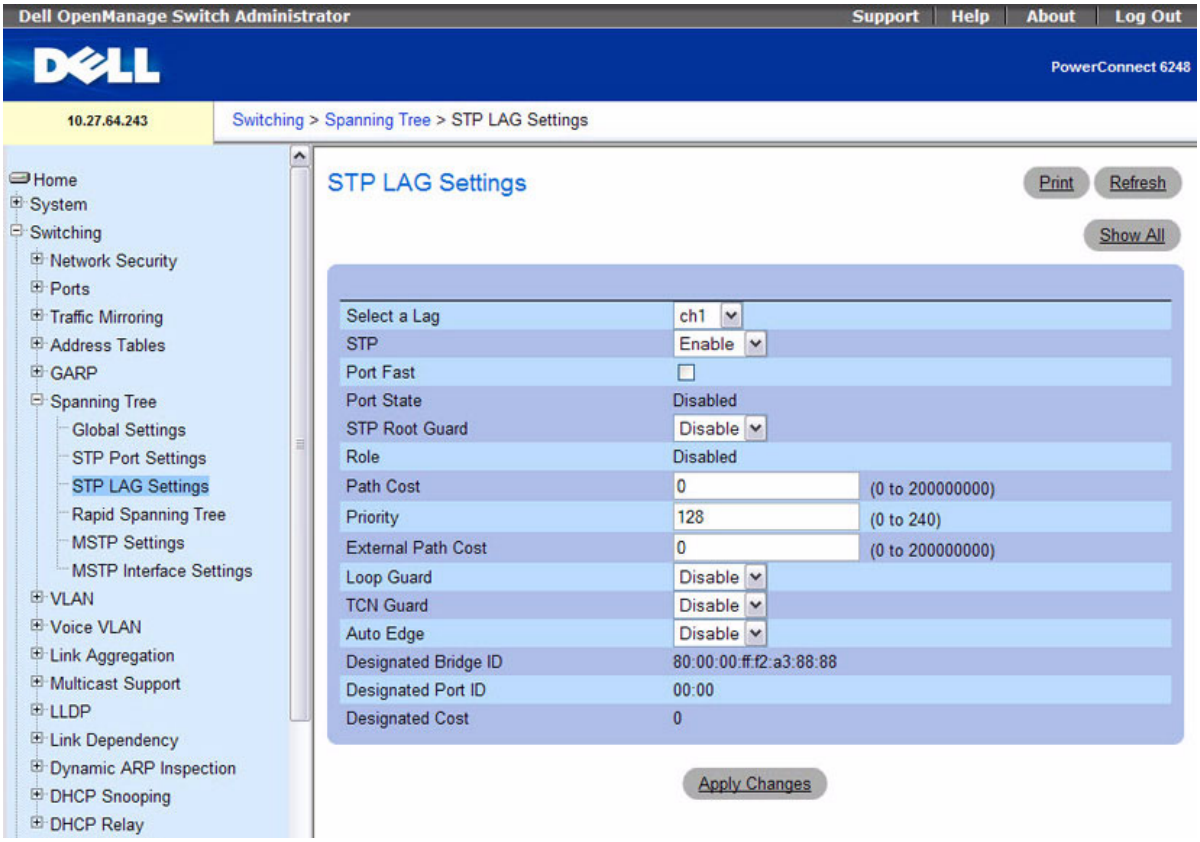
STP LAG Settings

Use the **STP LAG Settings** page to assign STP aggregating ports parameters.

To display the **STP LAG Settings** page, click **Switching > Spanning Tree > STP LAG Settings** in the tree view.

Downloaded from www.Manualslib.com manuals search engine

Figure 7-41. STP LAG Settings



The **STP LAG Settings** page contains the following fields:

- **Select a LAG** — Specifies the LAG number for which you want to modify STP settings.
- **STP** — Enables or disables STP on the LAG. Default is enable.
- **Port Fast** — Enables Port Fast mode for the LAG. If Port Fast mode is enabled for a LAG, the **Port State** is automatically placed in the **Forwarding** state when the LAG is up. Port Fast mode optimizes the time it takes for the STP protocol to converge. STP convergence can take 30–60 seconds in large networks.
- **Port State** — Displays current STP state of a LAG. If enabled, the LAG state determines what forwarding action is taken on traffic. If the bridge discovers a malfunctioning LAG, the LAG is placed in the **Broken** state. Possible LAG states are:
  - **Disabled** — STP is currently disabled on the LAG. The LAG forwards traffic while learning MAC addresses.
  - **Blocking** — The LAG is blocked and cannot be used to forward traffic or learn MAC addresses.
  - **Listening** — The LAG is in the listening mode and cannot forward traffic or learn MAC addresses.

Downloaded from www.Manualslib.com manuals search engine

- **Learning** — The LAG is in the learning mode and cannot forward traffic, but it can learn new MAC addresses.
- **Forwarding** — The LAG is currently in the forwarding mode, and it can forward traffic and learn new MAC addresses.
- **Broken** — The LAG is currently malfunctioning and cannot be used for forwarding traffic.

- **STP Root Guard** — Enables or disables STP Root Guard. The default is disable.
- **Role** — Displays the role this port has in the STP topology.
- **Path Cost** — Specifies amount the LAG contributes to the root path cost. The path cost is adjusted to a higher or lower value, and is used to forward traffic when a path is being rerouted. The range is 0–200000000. The default is 0.
- **Priority** — Specifies priority value of the LAG. The priority value influences the LAG choice when a bridge has two looped ports. The priority value is between 0–240. The default value is 128.
- **External Path Cost** — Specifies the External Path Cost to a new value for the specified port in the spanning tree. Enter 0 to set the external path cost value automatically on the basis of Link Speed. The default value is 0.
- **Loop Guard** — Prevents a LAG from erroneously transitioning from blocking state to forwarding when the LAG stops receiving BPDUs. The LAG is marked as being in loop-inconsistent state. In this state, the LAG does not forward packets. The possible values are Enable or Disable.
- **TCN Guard** — Enabling the TCN Guard feature restricts the LAG from propagating any topology change information received through that LAG. This means that even if a LAG receives a BPDU with the topology change flag set to true, the port will not flush its MAC address table and send out a BPDU with a topology change flag set to true.
- **Auto Edge** — Enabling the Auto Edge feature allows the LAG to become an edge port if it does not see BPDUs for some duration.
- **Designated Bridge ID** — Displays designated bridge ID.
- **Designated Port ID** — Displays designated port ID.
- **Designated Cost** — Displays cost of the port participating in the STP topology. Ports with a lower cost are less likely to be blocked if STP detects loops.

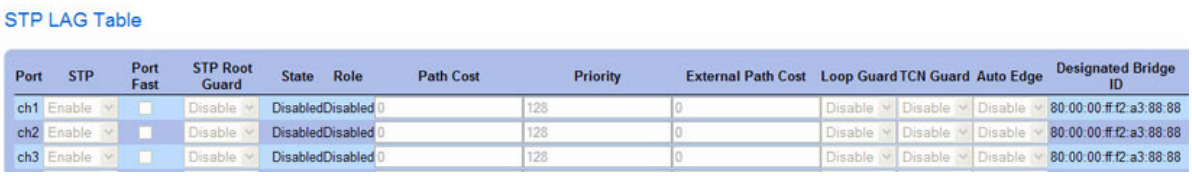
Displaying the STP LAG Table and Configuring STP LAG Settings

1. Open the **STP LAG Settings** page.
2. Click **Show All**.

   The **STP LAG Table** displays.

Downloaded from www.Manualslib.com manuals search engine

Figure 7-42. STP LAG Table



3. To change the STP settings for one or more LAGs, select the Edit option for the LAG(s), configure the desired settings, and then click **Apply Changes**.

Defining STP LAG Settings Using CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

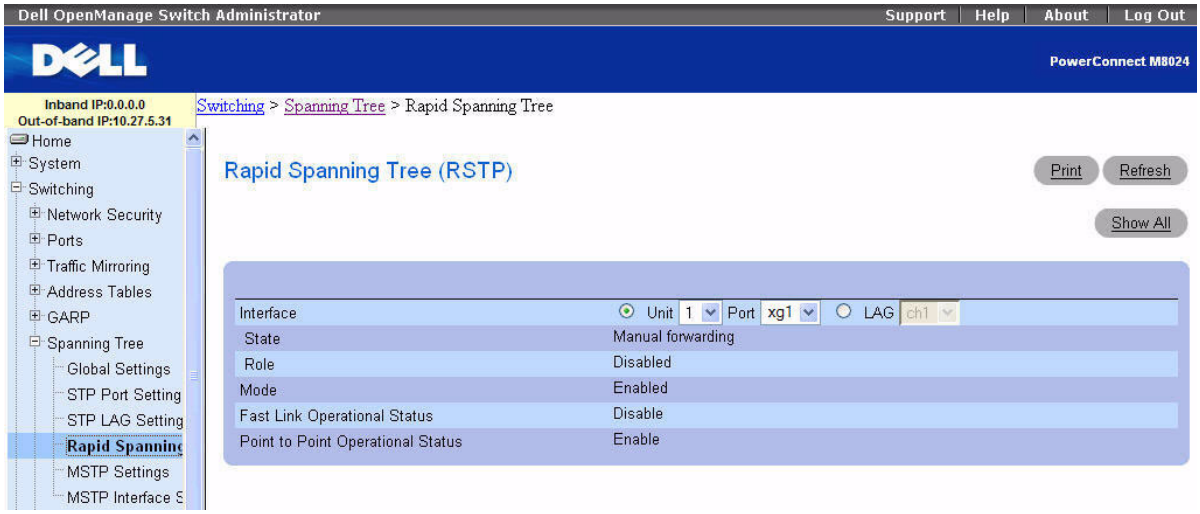
- Spanning Tree Commands

Rapid Spanning Tree

Rapid Spanning Tree Protocol (RSTP) detects and uses network topologies that allow a faster convergence of the spanning tree without creating forwarding loops.

To display the **Rapid Spanning Tree** page, click **Switching > Spanning Tree > Rapid Spanning Tree** in the tree view.

Figure 7-43. Rapid Spanning Tree



The **Rapid Spanning Tree** page contains the following fields:

- **Interface** — Determines if RSTP is enabled on a Unit/Port or on a LAG. Click Unit/Port or LAG to specify the type of interface, then select the Unit/Port or LAG to configure from the drop-down menu.
- **State** — Displays the spanning tree state for the port.

Downloaded from www.Manualslib.com manuals search engine

- **Role** — Displays the spanning tree role for the port in the STP topology.
- **Mode** — Displays the administrative mode and if its enabled or disabled.
- **Fast Link Operational Status** — Indicates if Fast Link is enabled or disabled for the port or LAG. If Fast Link is enabled for a port, the port is automatically placed in the forwarding state. This setting can be changed from the "STP Port Settings" or "STP LAG Settings" page.
- **Point to Point Operational Status** — Displays the Point-to-Point operating state.

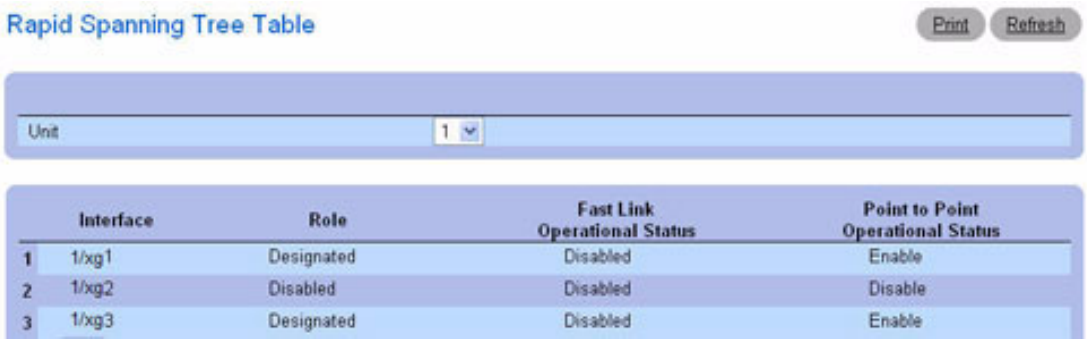
  To establish communications over a point-to-point link, the originating PPP first sends Link Control Protocol (LCP) packets to configure and test the data link. After a link is established and optional facilities are negotiated as needed by the LCP, the originating PPP sends Network Control Protocols (NCP) packets to select and configure one or more network layer protocols. When each of the chosen network layer protocols has been configured, packets from each network layer protocol can be sent over the link. The link remains configured for communications until explicit LCP or NCP packets close the link, or until some external event occurs. This is the actual switch port link type.

Displaying the Rapid Spanning Tree (RSTP) Table

1. Open the **Rapid Spanning Tree (RSTP)** page.
2. Click **Show All**.

   The **Rapid Spanning Tree Table** displays.

Figure 7-44. Rapid Spanning Tree Table



	Interface	Role	Fast Link Operational Status	Point to Point Operational Status
1	1/xg1	Designated	Disabled	Enable
2	1/xg2	Disabled	Disabled	Disable
3	1/xg3	Designated	Disabled	Enable

3. Use the **Unit** drop-down menu to view the **Rapid Spanning Tree Table** for other units in the stack, if they exist.

Defining Rapid STP Parameters Using the CLI Command

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- Spanning Tree Commands

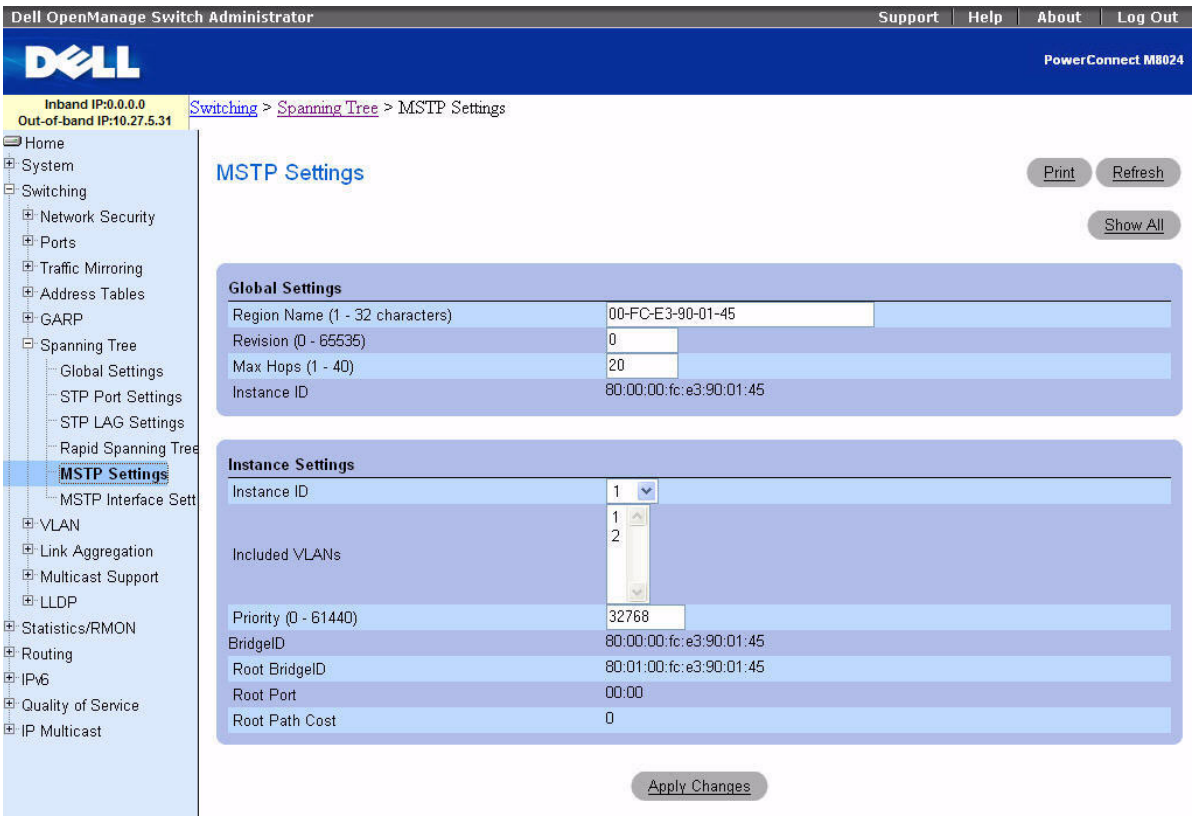
Downloaded from www.Manualslib.com manuals search engine

MSTP Settings

The Multiple Spanning Tree Protocol (MSTP) supports multiple instances of Spanning Tree to efficiently channel VLAN traffic over different interfaces. MSTP is compatible with both RSTP and STP; a MSTP bridge can be configured to behave entirely as a RSTP bridge or a STP bridge.

To display the **MSTP Settings** page, click **Switching > Spanning Tree > MSTP Settings** in the tree view.

Figure 7-45. MSTP Settings



The **MSTP Settings** page contains the following fields divided into two sections, **Global Settings** and **Instance Settings**:

- **Region Name (1–32 characters)** — Specifies a user-defined MST region name.
- **Revision (0–65535)** — Specifies unsigned 16-bit number that identifies the revision of the current MST configuration. The revision number is required as part of the MST configuration. Default is 0.
- **Max Hops (1–40)** — Specifies the total number of hops that occur in a specific region before the BPDU is discarded. Once the BPDU is discarded, the port information is aged out. Default is 20.
- **Instance ID** — Specifies the ID of the spanning tree instance. The field range is 1–15, and default is 1.

Downloaded from www.Manualslib.com manuals search engine

- **Included VLANs** — Maps the selected VLANs to the selected instance. Every VLAN belongs to one instance only.
- **Priority (0–61440) —** Specifies the switch priority for the selected spanning tree instance. The default value is 32768.
- **Bridge ID** — Indicates the bridge ID of the selected instance.
- **Root Bridge ID** of the root bridge which is the one with the lowest path cost.
- **Root Port —** Indicates the root port of the selected instance.
- **Root Path Cost —** Indicates the path cost of the selected instance.

Modifying MSTP Settings:

1. Open the **MSTP Settings** page.
2. Modify the fields in the **Global Settings** and **Instance Settings** sections as needed.
3. Click **Apply Changes**.

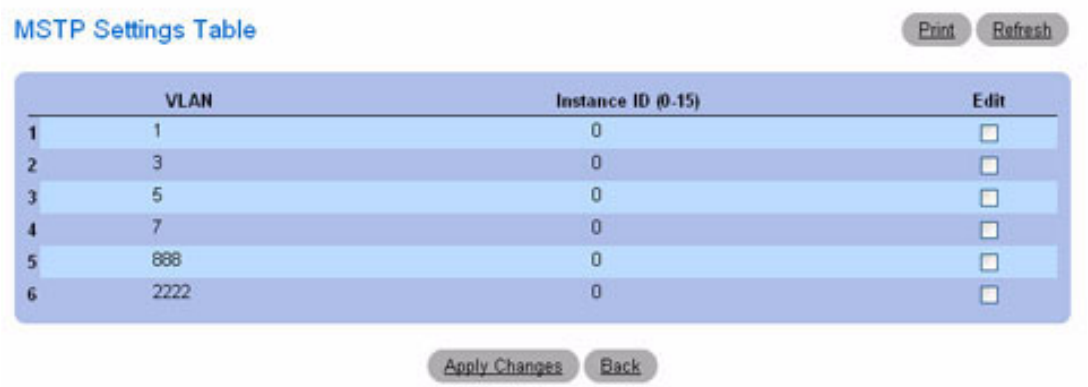
   The MSTP parameters are modified, and the device is updated.

Displaying the MSTP VLAN to Instance Mapping Table

1. Open the **MSTP Settings** page.
2. Click **Show All**.

   The **MSTP Settings Table** displays.

Figure 7-46. MSTP Settings Table



3. To modify the Instance ID for one or more VLANs, check **Edit** for the desired VLANs.
4. Make needed changes to Instance IDs. Enter a value of 0 to remove the VLAN-to-Instance mapping.
5. Click Apply Changes.

   The Instance IDs are modified for the selected VLANs, and the device is updated.

Downloaded from www.Manualslib.com manuals search engine

Defining MST Instances Using CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

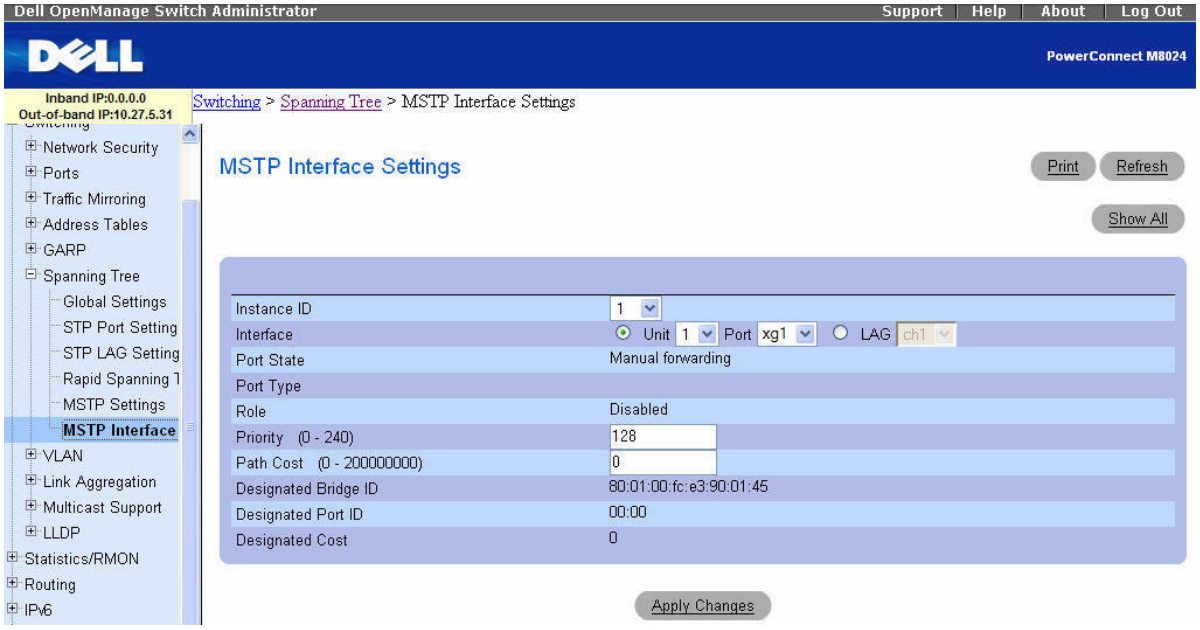
- Spanning Tree Commands

MSTP Interface Settings

Use the **MSTP Interface Settings** page to assign MSTP settings to specific interfaces.

To display the **MSTP Interface Settings** page, click **Switching > Spanning Tree > MSTP Interface Settings** in the tree view.

Figure 7-47. MSTP Interface Settings



The **MSTP Interface Settings** page contains the following fields:

- **Instance ID —** Selects the MSTP instances configured on the switch. Possible field range is 1–15.
- **Interface —** Selects either a Unit/Port or LAG for this MSTP instance.
- **Port State —** Indicates whether the port is enabled or disabled in the specific instance.
- **Port Type —** Indicates whether MSTP treats the port as a point-to-point port or a port connected to a hub and whether the port is internal to the MST region or a boundary port. If the port is a boundary port, it also indicates whether the switch on the other side of the link is working in RSTP or STP mode
- **Role —** Indicates the port role assigned by the STP algorithm in order to provide to STP paths. The possible field values are:
  - **Root** — Provides the lowest cost path to forward packets to root switch.

Downloaded from www.Manualslib.com manuals search engine

- **Designated** — Indicates the port or LAG through which the designated switch is attached to the LAN.
- **Alternate** — Provides an alternate path to the root switch from the interface.
- **Backup** — Provides a backup path to the designated LAN. Backup ports occur only when two ports are connected in a loop by a point-to-point link. Backup ports also occur when a LAN has two or more connections connected to a shared segment.
- **Disabled** — Indicates the port is not participating in the Spanning Tree.

- **Priority —** Defines the interface priority for the specified instance. The priority range is 0–240 in steps of 16. The default value is 128.
- **Path Cost (0–200000000)** — Indicates the port contribution to the Spanning Tree instance. The range should always be 0–200,000,000. The default value is determined by the port's speed. The default value is:
  - Port Channel-20,000
  - 1000 mbps (giga)-20,000
  - 100 mbps-200,000
  - 10 mbps-2,000,000
- **Designated Bridge ID —** Displays the bridge ID number that connects the link or shared LAN to the root.
- **Designated Port ID —** Displays the port ID number on the designated bridge that connects the link or the shared LAN to the root.
- **Designated Cost —** Displays cost of the path from the link or the shared LAN to the root.

Assigning MSTP Interface Settings

1. Open the **MSTP Interface Settings** page.
2. Select an **Instance ID** from the drop-down menu.
3. Specify **Port** or **LAG**, then select the interface from the related drop-down menu.
4. Specify **Interface Priority** and **Path Cost**.
5. Click **Apply Changes**.

   The interface settings are saved, and the device is updated.

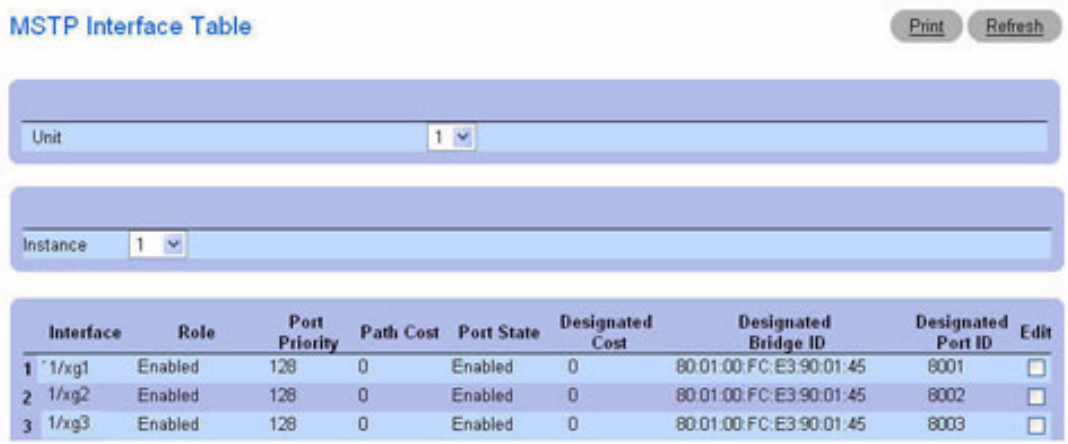
Displaying the MSTP Interface Settings Table

1. Open the **MSTP Settings** page.
2. Click **Show All**.

   The **MSTP Interface Table** displays.

Downloaded from www.Manualslib.com manuals search engine

Figure 7-48. MSTP Interface Table



3. Use the **Unit** drop-down menu to view the **MSTP Interface Table** for other units in the stack, if they exist.
4. To modify the port priority or path cost for one or more interfaces, check **Edit** for the desired interfaces.
5. Make the needed changes to the values in the **Port Priority** or **Path Cost** columns.
6. Click Apply Changes.

   The fields are modified for the selected Interfaces, and the device is updated.

Defining MSTP Interfaces Using CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- Spanning Tree Commands

Configuring VLANs

Adding Virtual LAN (VLAN) support to a Layer 2 switch offers some of the benefits of both bridging and routing. Like a bridge, a VLAN switch forwards traffic based on the Layer 2 header, which is fast, and like a router, it partitions the network into logical segments, which provides better administration, security and management of multicast traffic.

A VLAN is a set of end stations and the switch ports that connect them. You may have many reasons for the logical division, such as department or project membership. The only physical requirement is that the end station and the port to which it is connected both belong to the same VLAN.

Downloaded from www.Manualslib.com manuals search engine

Each VLAN in a network has an associated VLAN ID, which appears in the IEEE 802.1Q tag in the Layer 2 header of packets transmitted on a VLAN. An end station may omit the tag, or the VLAN portion of the tag, in which case the first switch port to receive the packet may either reject it or insert a tag using its default VLAN ID. A given port may handle traffic for more than one VLAN, but it can only support one default VLAN ID.

To display the **VLAN** menu page, click **Switching > VLAN** in the tree view. This **VLAN** page contains links to the following features:

- VLAN Membership
- Double VLAN
- VLAN Port Settings
- VLAN LAG Settings
- Bind MAC to VLAN
- Bind IP Subnet to VLAN
- Protocol Group
- GVRP Parameters

VLAN Membership

Use the **VLAN Membership** page to define VLAN groups stored in the VLAN membership table. Your switch supports up to 4094 VLANs. However, you can actually create only 4092 VLANs because:

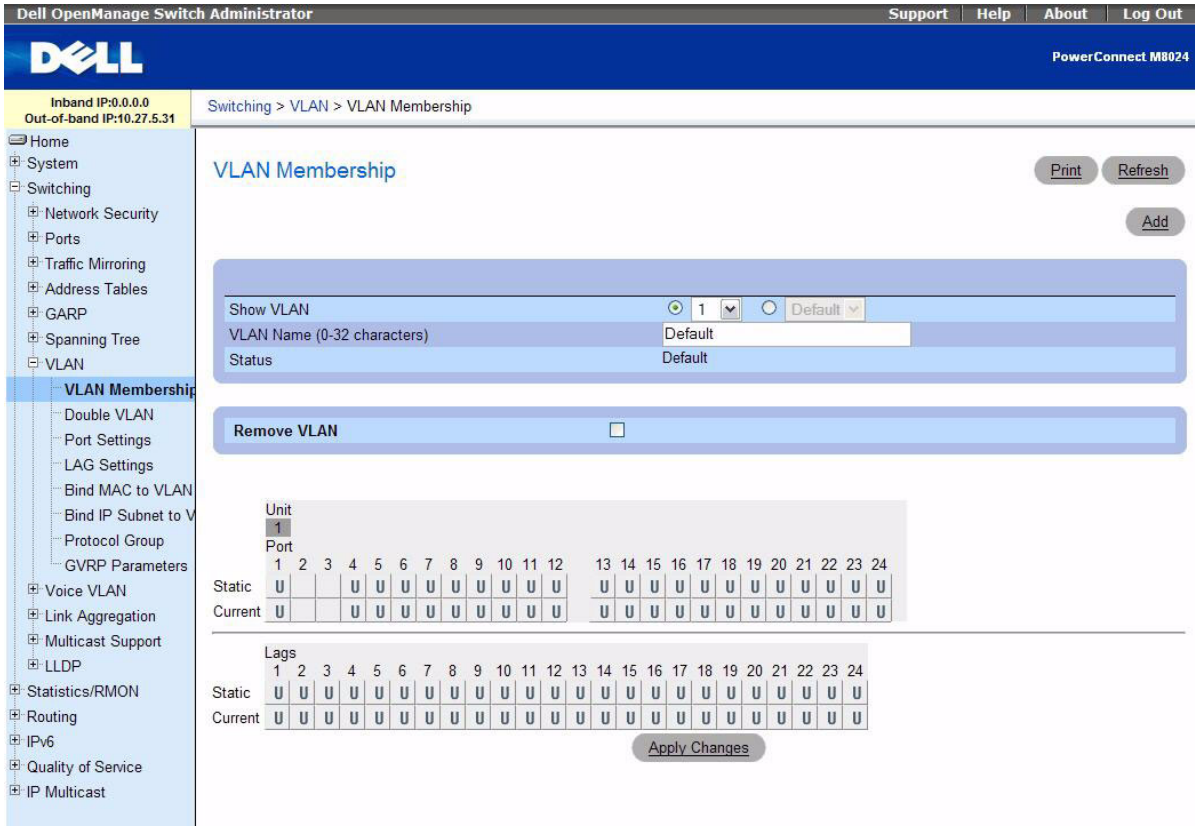
- VLAN 1 is the default VLAN of which all ports are members, and
- VLAN 4095 is designated as the "Discard VLAN."

Valid VLANs that can be created are 2–4093. VLAN 4094 is reserved.

To display the **VLAN Membership** page, click **Switching > VLAN > VLAN Membership** in the tree view.

Downloaded from www.Manualslib.com manuals search engine

Figure 7-49. VLAN Membership



The **VLAN Membership** page is divided into two sections. The top section contains fields that define the entire VLAN's membership. The bottom section contains tables that define membership settings for specific Ports and LAGs on this VLAN. Following are the **VLAN Membership** fields:

- **Show VLAN** — Selects the VLAN to display. Use either the **VLAN ID** or **VLAN Name** drop-down menu to select the VLAN.
- **VLAN Name (0–32)** — Indicates the user-defined VLAN name. This field is defined using the **Add** button. Valid names can range from 0–32 characters in length.
- **Status**—Indicates the VLAN type. Possible values are:
  - **Dynamic** — Indicates the VLAN was dynamically created through GVRP.
  - **Static** — Indicates the VLAN is user-defined and may be modified.
  - **Default** — Indicates the VLAN is the default VLAN.
- **Remove VLAN** — Removes the displayed VLAN from the VLAN Membership Table when checked.

The **VLAN Membership** tables display which Ports and LAGs are members of the VLAN, and whether they're tagged (T), untagged (U), or forbidden (F). The tables have two rows: **Static** and **Current**. Only the **Static** row is accessible from this page. The **Current** row is updated either dynamically through GVRP or when the **Static** row is changed and **Apply Changes** is clicked.

Downloaded from www.Manualslib.com manuals search engine

There are two tables in this section of the page:

- **Ports** — Displays and assigns VLAN membership to ports. To assign membership, click in **Static** for a specific port. Each click toggles between U, T, and blank. See the following table for definitions.
- **LAGs** — Displays and assigns VLAN membership to LAGs. To assign membership, click in **Static** for a specific LAG. Each click toggles between U, T, and blank. See the following table for definitions.

Table 7-1. VLAN Port Membership Definitions

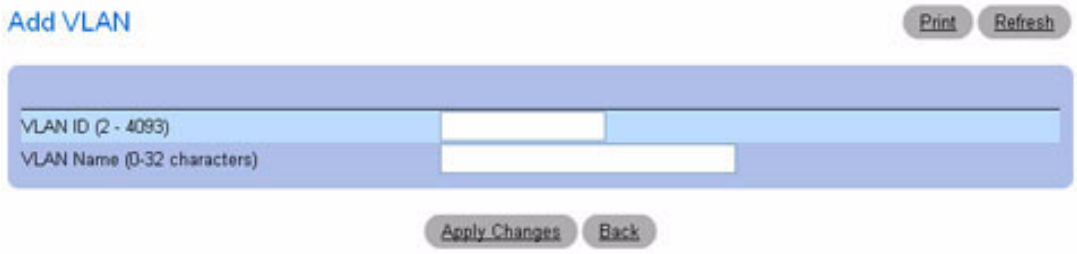
Port Control	Definition
T	Tagged: the interface is a member of a VLAN. All packets forwarded by the interface are tagged. The packets contain VLAN information.
U	Untagged: the interface is a VLAN member. Packets forwarded by the interface are untagged.
F	Forbidden: indicates that the interface is forbidden from becoming a member of the VLAN.
Blank	Blank: the interface is not a VLAN member. Packets associated with the interface are not forwarded.

Adding New VLANs

1. Open the **VLAN Membership** page.
2. Click **Add**.

   The **Add VLAN** page displays.

Figure 7-50. Add VLAN



3. Enter a new VLAN ID and VLAN Name.
4. Click **Apply Changes**.

   The new VLAN is added, and the device is updated.

Downloaded from www.Manualslib.com manuals search engine

Assigning VLAN Membership to a Port or LAG

1. Open the **VLAN Membership** page.
2. Select a VLAN from the **VLAN ID** or **VLAN Name** drop-down menu.
3. In the **VLAN Port Membership Table**, assign a value by clicking in the **Static** row for a specific Port/LAG. Each click toggles between U, T, and blank (not a member).
4. Click **Apply Changes**.

   The Port or LAG is assigned to the VLAN with the selected designation, the **Current** row is updated with the designation, and the device is updated.

Modifying VLAN Membership Groups

1. Open the **VLAN Membership** page.
2. Select a VLAN from the **VLANID** or **VLAN Name** drop-down menu.
3. Modify the fields as needed.
4. In the **VLAN Port Membership Table**, change a Port or LAG value by clicking in the **Static** row for that Port/LAG. Each click toggles between U, T, and blank (not a member).
5. Click **Apply Changes**.

   The VLAN membership information is modified, the **Current** row is updated with any changes in designation, and the device is updated.

Removing a VLAN

1. Open the **VLAN Membership** page.
2. Select a VLAN from the **VLAN ID** or **VLAN Name** drop-down menu.
3. Check the **Remove VLAN** check box.
4. Click **Apply Changes**.

   The selected VLAN is removed, and the device is updated.

Defining VLAN Membership Groups and Assigning Ports/LAGs Using CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- VLAN Commands

Double VLAN

The Double VLAN feature allows the use of a second tag on network traffic. The additional tag helps differentiate between customers in the Metropolitan Area Networks (MAN) while preserving individual customer's VLAN identification when they enter their own 802.1Q domain.

With the introduction of this second tag, you do not need to divide the 4k VLAN ID space to send traffic on an Ethernet-based MAN.

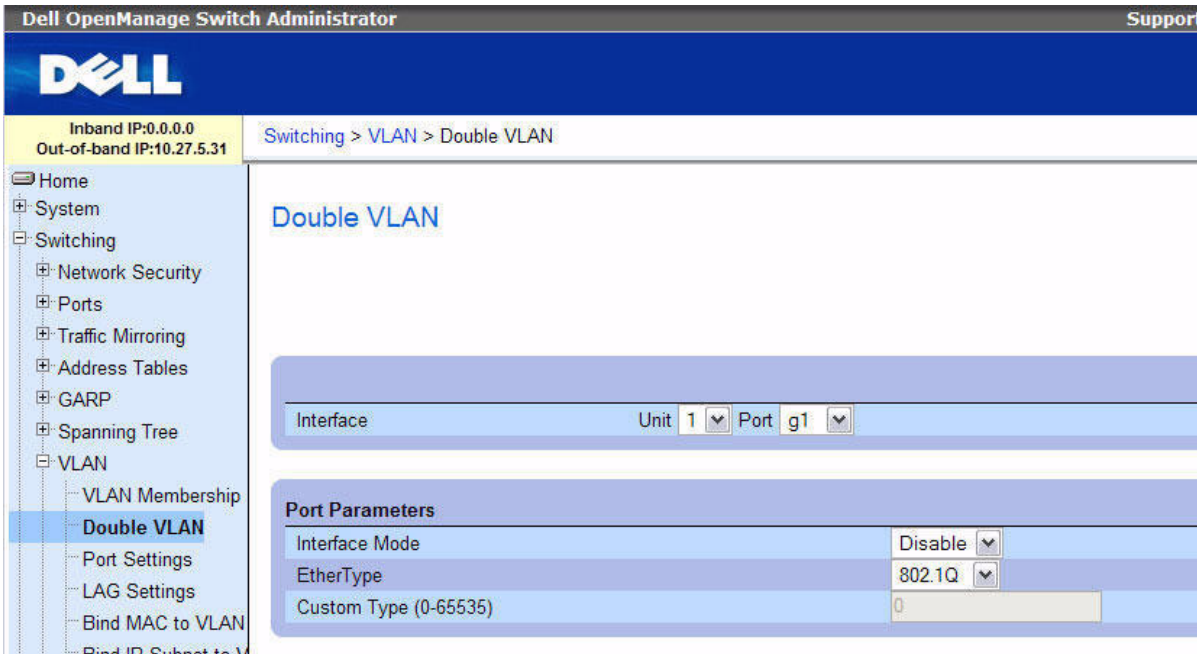
Downloaded from www.Manualslib.com manuals search engine

With Double VLAN Tunneling enabled, every frame that is transmitted from an interface has a DVLAN Tag attached while every packet that is received from an interface has a tag removed (if one or more tags are present).

Use the **Double VLAN Global Configuration** page to specify the Double VLAN configuration for all the ports.

To access the **Double VLAN** Global Configuration page, click **Switching > VLAN > Double VLAN > Global Configuration** from the navigation tree.

Figure 7-51. Double VLAN Global Configuration



The **Double VLAN Global Configuration** page contains the following fields:

- **EtherType** — The two-byte hex Ethertype to be used as the first 16 bits of the Double VLAN tag:
  - **802.1Q** — Commonly used tag representing 0x8100. This value is supported by several network equipment manufacturers. If a double-tagged frame with the first Ethertype value set to 802.1Q is forwarded to hardware which does not support Double VLAN (or the corresponding configuration is not set), it will be misinterpreted as a regular, single-tagged frame.
  - **vMAN** — Commonly used tag representing 0x88A8, defined for the Virtual Metropolitan Area Network. This value is often used to indicate double-tagged frames. If a double-tagged frame with an Ethertype value set to vMAN is forwarded to hardware without Double VLAN support (or when Double VLAN is not configured), it will be dropped due to unknown Ethertype. This outcome may be more efficient, and cause less harm than when the 802.1Q Ethertype value is used for double-tagged frames. When presented with a double-tagged frame with an 802.1Q Ethertype value, the switch that does not support double-tagging may attempt to process the double-tagged frame with the incorrect assumption that frame contains only a single VLAN tag.

Downloaded from www.Manualslib.com manuals search engine

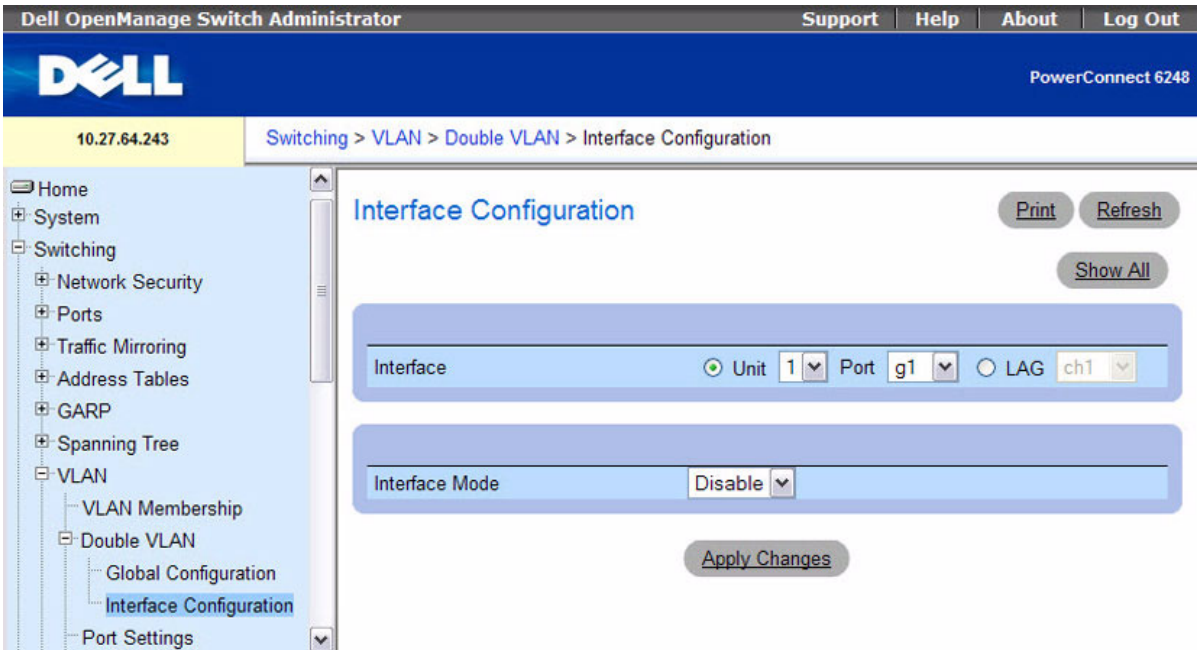
– **Custom** — Use this to specify that double-tagged frames will use a custom Ethertype. A custom Ethertype may be used to make the switch interoperable with specific or non-standard equipment that does not support 802.1 or vMAN values of Ethertype in double-tagged frames. For more information, refer to the list of registered Ethertype values for common protocols.

- **Custom Type** — If **Custom** is selected in the Ethertype field, enter a custom Ethertype value in any range from 0 to 65535.

Use the **Double VLAN Interface Configuration** page to enable or disable Double VLAN mode on a physical port or LAG.

To access the **Double VLAN** Interface Configuration page, click **Switching > VLAN > Double VLAN Interface Configuration** from the navigation tree.

Figure 7-52. Double VLAN Interface Configuration



Downloaded from www.Manualslib.com manuals search engine

The **Double VLAN Interface Configuration** page contains the following fields:

- **Interface** — Select the port or LAG for which you want to display or configure data.
- **Interface Mode** — Enables or disables double VLAN tagging on the selected interface. The default value is **Disable**.

Assigning Double VLAN Tags

1. Open the **Double VLAN Global Configuration** page.
2. Select the **Ethertype** from the drop-down menu.
3. Click **Apply Changes**.
4. Open the **Double VLAN Interface Configuration** page.
5. Select the port to which you want to assign settings from the **Interface** drop-down menu.
6. Select the **Interface Mode** from the drop-down menu.
7. Click **Apply Changes**.

   The Double VLAN settings are defined, and the device is updated.

Displaying the Double VLAN Port Parameters Table

1. Open the **Double VLAN Interface Configuration** page.
2. Click **Show All**.

   The **Double VLAN Port Parameters Table** displays.

Figure 7-53. Double VLAN Port Parameters Table

Downloaded from www.Manualslib.com manuals search engine

Copying Double VLAN Parameters

1. Open the **Double VLAN Interface Configuration** page.
2. Click **Show All**.

   The **Double VLAN Port Parameters Table** displays.
3. Specify the Port you are copying from in **Copy Parameters From**.
4. Click **Copy To** for each Interface to receive these parameters.
5. Click **Apply Changes**.

   The Double VLAN port settings are copied, and the device is updated.

Modifying Settings for Multiple Ports

1. Open the **Double VLAN Interface Configuration** page.
2. Click **Show All**.

   The **Double VLAN Port Parameters Table** displays.
3. Click **Edit** for each Port to modify.
4. Edit fields as needed.
5. Click **Apply Changes**.

   The Double VLAN port settings are modified, and the device is updated.

Configuring Double VLAN Tagging Using CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- VLAN Commands

VLAN Port Settings

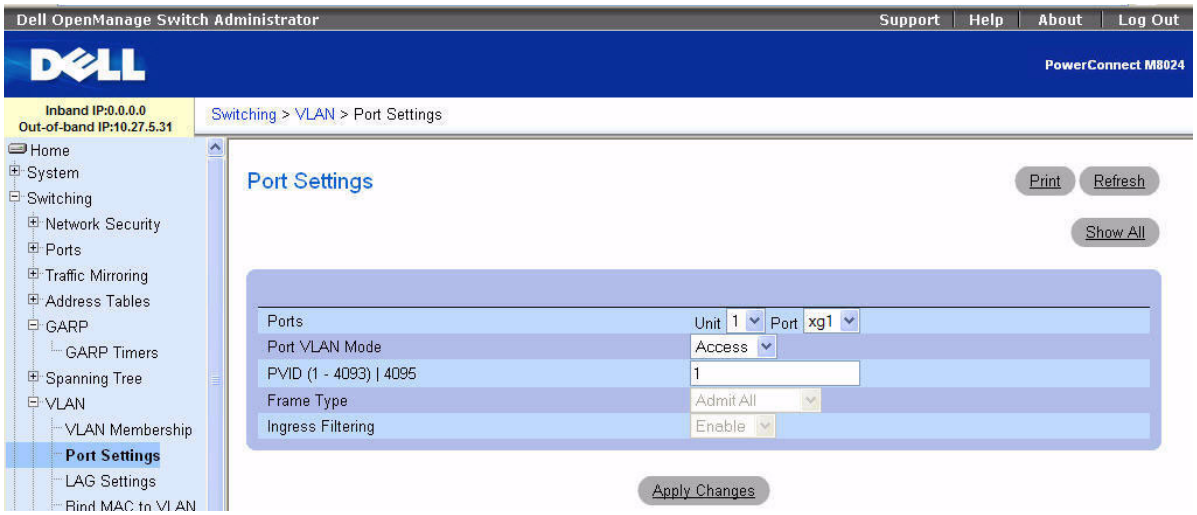
In a port-based VLAN, untagged traffic is bridged through specified ports based on the receiving ports PVID. Port-based VLANs can help optimize network traffic patterns because broadcast, multicast, and unknown unicast packets are sent only to ports that are members of the VLAN. Packets that are received with a VLAN tag uses that VLAN ID for the switching process.

Use the **VLAN Port Settings** page to identify a port as part of a VLAN, as well as to define and modify VLAN port parameters.

To display the **VLAN Port Settings** page, click **Switching > VLAN > Port Settings** in the tree view.

Downloaded from www.Manualslib.com manuals search engine

Figure 7-54. VLAN Port Settings



The **VLAN Port Settings** page contains the following fields:

- **Ports** — Specifies the Unit and Port included in the VLAN.
- **Port VLAN Mode** — Indicates the port mode. Possible values are:
  - **General** — The port belongs to VLANs, and each VLAN is user-defined as tagged or untagged (full 802.1Q mode).
  - **Access** — The port belongs to a single untagged VLAN. When a port is in Access mode, the packet types which are accepted on the port (packet type) cannot be designated. It is also not possible to enable/disable ingress filtering on an access port.
  - **Trunk** — The port belongs to more than one VLAN, and all ports are tagged (except for an optional single native VLAN).
- **PVID (1–4093) | 4095** — Assigns a VLAN ID to untagged packets. Possible values are 1–4093 or 4095.
- **Frame Type** — Specifies frame type accepted on the port. Default is **Admit All**. Possible values are:
  - **Admit Tag Only**—Indicates that only tagged frames are accepted on the port.
  - **Admit All**—Indicates that both tagged and untagged frames are accepted on the port.
- **Ingress Filtering** — Enables or disables Ingress filtering on the port. Ingress filtering discards frames where the VLAN tag does not match the port VLAN membership.

Downloaded from www.Manualslib.com manuals search engine

Assigning Port Settings

1. Open the **VLAN Port Settings** page.
2. Select the port to which you want to assign settings from the **Unit** and **Port** drop-down menus.
3. Complete the remaining fields on the page.
4. Click **Apply Changes**.

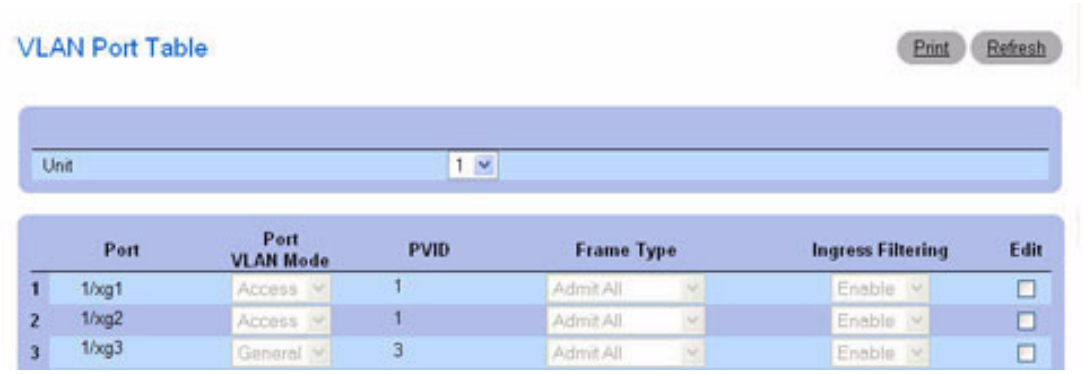
   The VLAN port settings are defined, and the device is updated.

Displaying the VLAN Port Table

1. Open the **VLAN Port Settings** page.
2. Click **Show All**.

   The **VLAN Port Table** displays.

Figure 7-55. VLAN Port Table



Note: If an **Access** port is chosen, the packet types that are accepted on the port (packet type) cannot be designated. It is also not possible to enable or disable ingress filtering on an access port.

3. Use the **Unit** drop-down menu to view the **VLAN Port Table** for other units in the stack, if they exist.

Modifying Settings for Multiple Ports

1. Open the **VLAN Port Settings** page.
2. Click **Show All**.

   The **VLAN Port Table** displays.
3. Click **Edit** for each Port to modify.
4. Edit fields as needed.
5. Click **Apply Changes**.

   The VLAN port settings are modified, and the device is updated.

Downloaded from www.Manualslib.com manuals search engine

Assigning Ports to VLAN Groups Using CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

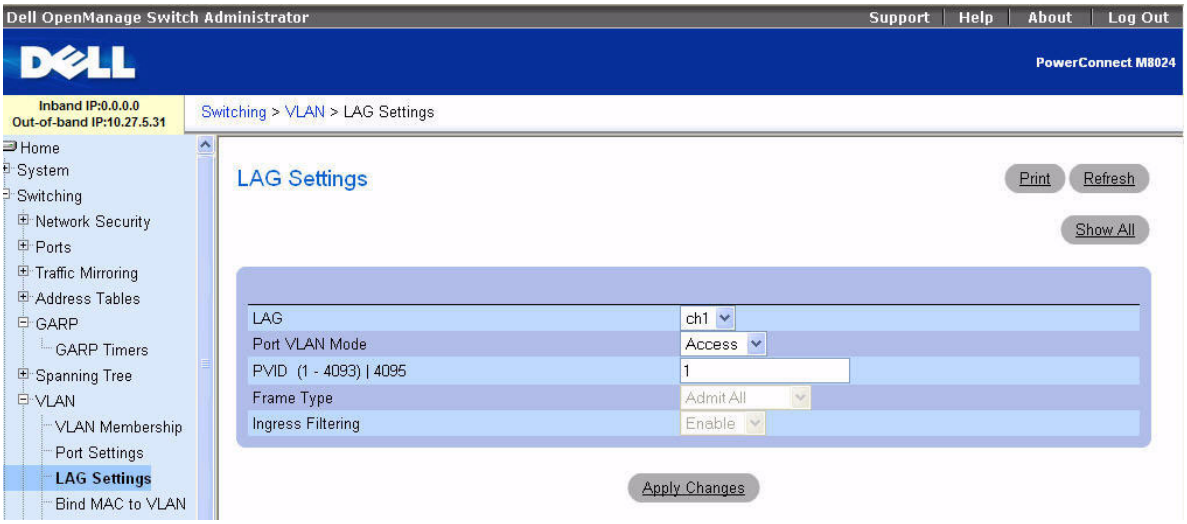
- VLAN Commands

VLAN LAG Settings

Use the **VLAN LAG Settings** page to map a LAG to a VLAN. Untagged packets entering the switch are tagged with the LAGs ID specified by the PVID.

To display the **VLAN LAG Settings** page, click **Switching > VLAN > LAG Settings** in the tree view.

Figure 7-56. VLAN LAG Settings



The **VLAN LAG Settings** page contains the following fields:

- **LAG** — Specifies the LAG number included in the VLAN.
- **Port VLAN Mode** — Indicates the Port VLAN mode for the LAG. Possible values are:
  - **General** — The LAG belongs to VLANs, and each VLAN is user-defined as tagged or untagged (full 802.1Q mode).
  - **Access** — The LAG belongs to a single, untagged VLAN.
- **Trunk** — The LAG belongs to more than one VLAN, and all ports are tagged (except for an optional single native VLAN).
- **PVID (1–4093) | 4095** — Assigns a VLAN ID to untagged packets. The possible field values are 1–4093 or 4095.
- **Frame Type** — Specifies packet type accepted by the LAG. Admit Tag Only is the default. Possible values are:

Downloaded from www.Manualslib.com manuals search engine

– **Admit Tag Only** — The LAG only accepts tagged packets.

– **Admit All** — Tagged and untagged packets are both accepted by the LAG.

- **Ingress Filtering** — Enables or disables Ingress filtering by the LAG. Ingress filtering discards packets where the VLAN tag does not match the LAG VLAN membership.

Assigning VLAN LAG Settings

1. Open the **VLAN LAG Settings** page.
2. Select a LAG from the **LAG** drop-down menu
3. Complete the remaining fields on the page.
4. Click **Apply Changes**.

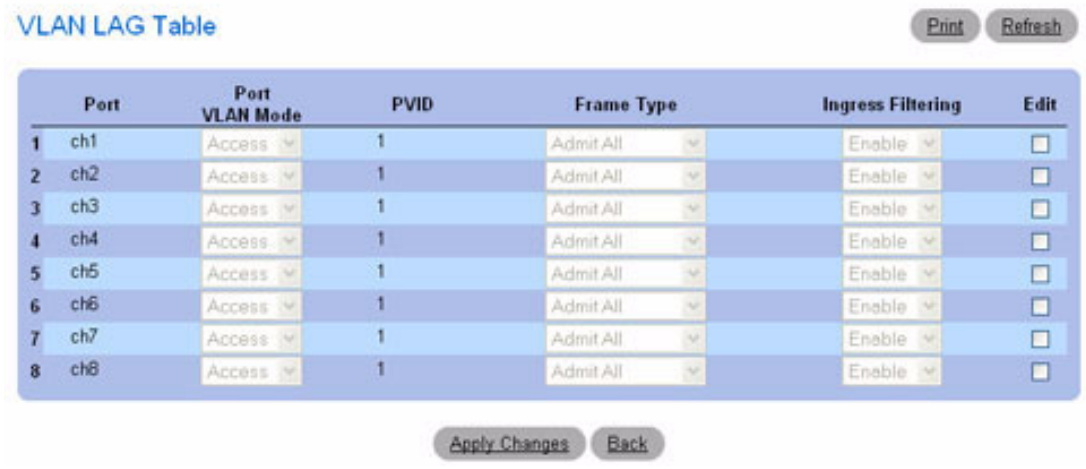
   The VLAN LAG parameters are defined, and the device is updated.

Displaying the VLAN LAG Table

1. Open the **VLAN LAG Settings** page.
2. Click **Show All**.

   The **VLAN LAG Table** displays.

Figure 7-57. VLAN LAG Table



Downloaded from www.Manualslib.com manuals search engine

Modifying Settings for Multiple LAGs

1. Open the **VLAN LAG Settings** page.
2. Click **Show All**.

   The **VLAN LAG Table** displays.
3. Click **Edit** for each LAG to modify.
4. Edit fields as needed.
5. Click **Apply Changes**.

   The VLAN LAG settings are modified, and the device is updated.

Assigning LAGs to VLAN Groups Using CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

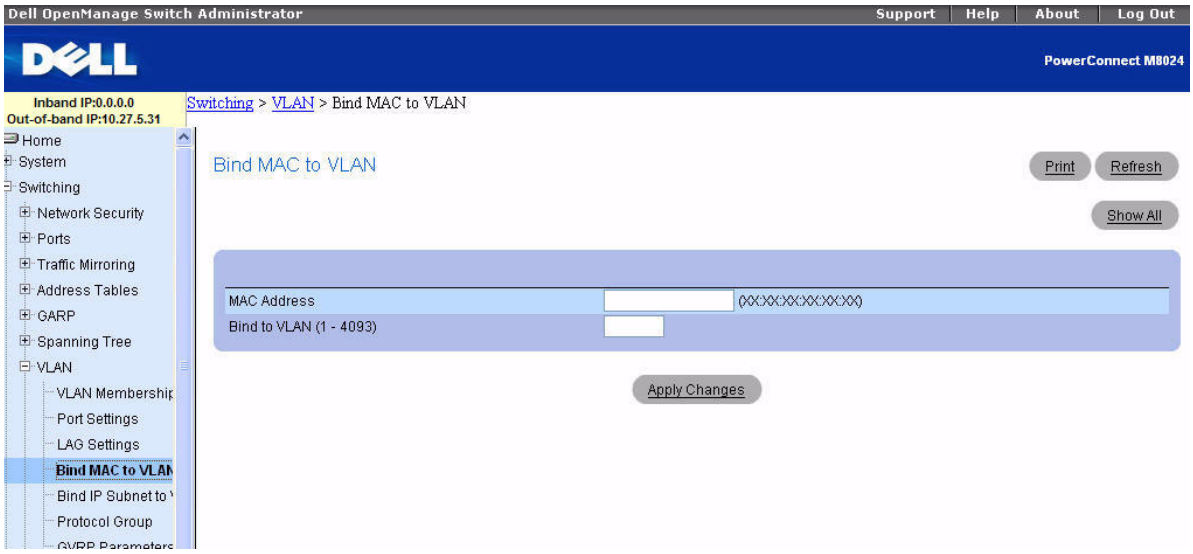
- VLAN Commands

Bind MAC to VLAN

Use the **Bind MAC to VLAN** page to map a MAC entry to the VLAN table. After the source MAC address and the VLAN ID are specified, the MAC to VLAN configurations are shared across all ports of the switch. The MAC to VLAN table supports up to 128 entries.

To display the **Bind MAC to VLAN** page, click **Switching > VLAN > Bind MAC to VLAN** in the tree view.

Figure 7-58. Bind MAC to VLAN



The **Bind MAC to VLAN** page contains the following fields:

Downloaded from www.Manualslib.com manuals search engine

- **MAC Address** — Specifies MAC Address for a VLAN.
- **Bind to VLAN** (1–4093) — Specifies VLAN to which the MAC is to be bound.

Assigning Bind MAC to VLAN Settings

1. Open the **Bind MAC to VLAN** page.
2. Enter the MAC Address to bind to the VLAN.
3. Enter the VLAN to which the MAC Address is to be bound.
4. Click **Apply Changes**.

   The listed MAC Address and VLAN are now bound, and the device is updated.

Displaying the VLAN LAG Table

1. Open the **Bind MAC to VLAN** page.
2. Click **Show All**.

   The **MAC - VLAN Bind Table** displays.

Figure 7-59. MAC - VLAN Bind Table

Modifying VLAN for Multiple MAC Addresses

1. Open the **Bind MAC to VLAN** page.
2. Click **Show All**.

   The **MAC - VLAN Bind Table** displays.
3. Click **Edit** for each MAC Address with a VLAN to modify.
4. Edit the **Bind to VLAN** fields.
5. Click **Apply Changes**.

   The MAC to VLAN settings are modified, and the device is updated.

Downloaded from www.Manualslib.com manuals search engine

Removing a MAC - VLAN Entry

1. Open the **Bind MAC to VLAN** page.
2. Click **Show All**.

   The **MAC - VLAN Bind Table** displays.
3. Check **Remove** for each entry to remove.
4. Click **Apply Changes**.

   The entry/entries are removed, and the device is updated.

Binding MACs to VLANs Using CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- VLAN Commands

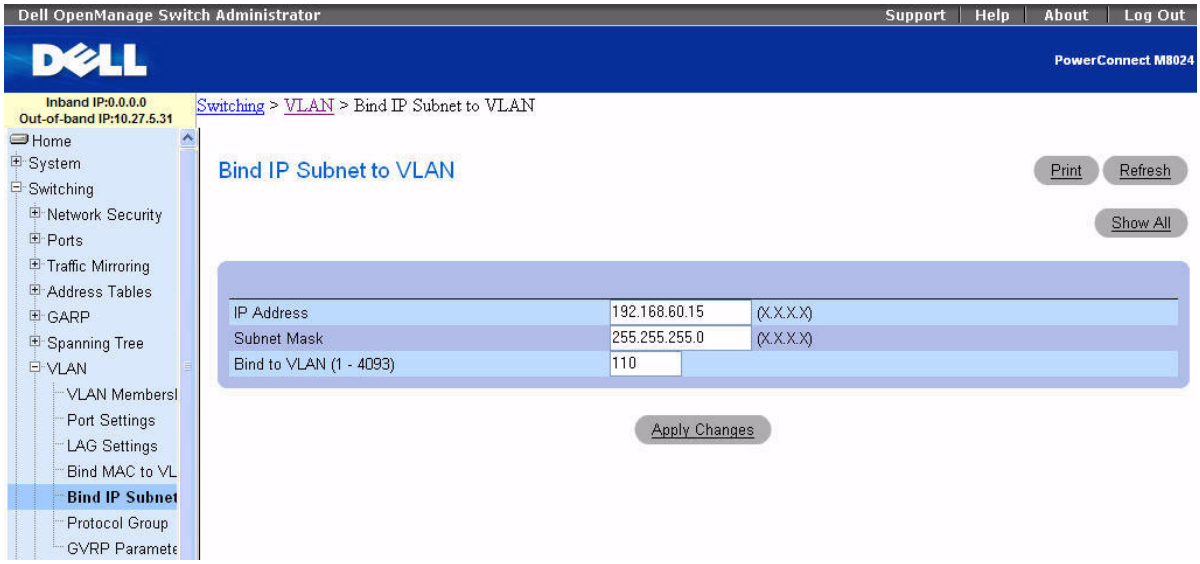
Bind IP Subnet to VLAN

An IP Subnet to VLAN mapping is defined by configuring an entry in the IP Subnet to VLAN table, an entry is specified through a source IP address, network mask, and the desired VLAN ID. The IP Subnet to VLAN configurations are shared across all ports of the switch. There can be up to 64 entries configured in this table.

Use the **Bind IP Subnet to VLAN** page to assign an IP Subnet to a VLAN.

To display the **Bind IP Subnet to VLAN** page, click **Switching > VLAN > Bind IP Subnet to VLAN** in the tree view.

Figure 7-60. Bind IP Subnet to VLAN



Downloaded from www.Manualslib.com manuals search engine

The **Bind IP Subnet to VLAN** page contains the following fields:

- **IP Address** — Specifies packet source IP address.
- **Subnet Mask** — Specifies packet source IP subnet mask.
- **Bind to VLAN (1–4093)** — Specifies VLAN to which the IP Address is assigned.

Binding an IP Subnet to a VLAN

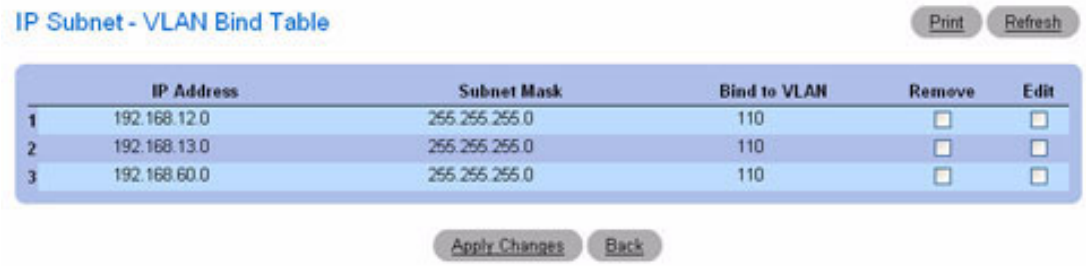
1. Open the **Bind IP Subnet to VLAN** page.
2. Enter the IP Address to bind to the VLAN.
3. Enter the IP Subnet associated with the IP address.
4. Enter the VLAN ID to which the IP address and subnet mask are assigned.
5. Click **Apply Changes**.

   The listed VLAN and IP Subnet are now bound, and the device is updated.

Displaying the IP Subnet - VLAN Bind Table

1. Open the **Bind IP Subnet to VLAN** page.
2. Click **Show All**.
3. The **IP Subnet - VLAN Bind Table** displays.

Figure 7-61. IP Subnet - VLAN Bind Table



	IP Address	Subnet Mask	Bind to VLAN	Remove	Edit
1	192.168.12.0	255.255.255.0	110	☐	☐
2	192.168.13.0	255.255.255.0	110	☐	☐
3	192.168.60.0	255.255.255.0	110	☐	☐

Modifying the VLAN Bound to Multiple IP Addresses

1. Open the **Bind IP Subnet to VLAN** page.
2. Click **Show All**.

   The **IP Subnet - VLAN Bind Table** displays.
3. Click **Edit** for each entry to modify.
4. Edit the fields as needed.
5. Click **Apply Changes**.

   The Bind to VLAN settings are modified, and the device is updated.

Downloaded from www.Manualslib.com manuals search engine

Removing a MAC - IP Subnet Entry

1. Open the **Bind IP Subnet to VLAN** page.
2. Click **Show All**.

   The **IP Subnet - VLAN Bind Table** displays.
3. Check **Remove** for each entry to remove.
4. Click **Apply Changes**.

   The entry/entries are removed, and the device is updated.

Binding IP Subnets to VLANs Using CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- VLAN Commands

Protocol Group

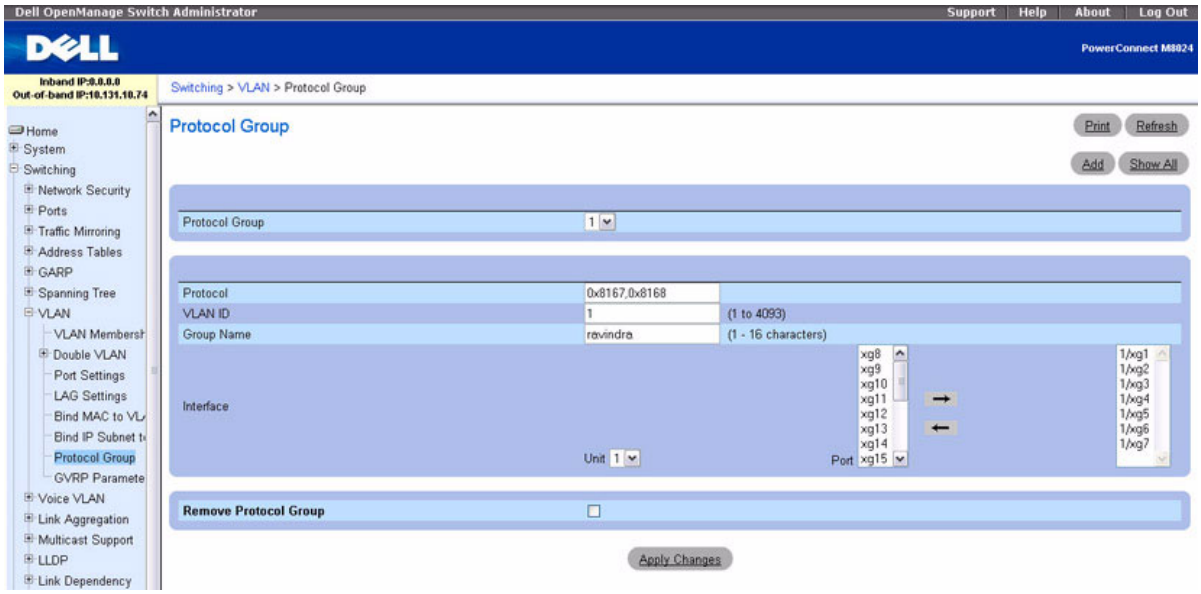
In a protocol-based VLAN, traffic is bridged through specified ports based on the VLAN's protocol. User-defined packet filters determine if a particular packet belongs to a particular VLAN. Protocol-based VLANs are most often used in situations where network segments contain hosts running multiple protocols.

Use the **Protocol Group** page to configure which EtherTypes go to which VLANs, and then enable certain ports to use these settings.

To display the **Protocol Group** page, click **Switching > VLAN > Protocol Group** in the tree view.

Downloaded from www.Manualslib.com manuals search engine

Figure 7-62. Protocol Group



The **Protocol Group** page contains the following fields:

- **Protocol Group** — Displays the name associated with the protocol group ID (up to 16 characters). Create a new group by clicking the **Add** button.
- **Protocol** — Specifies protocols (in hexadecimal format in the range 0x0600 to 0xffff) associated with this group. Enter up to 16 protocols using comma separated list.
- **VLAN ID (1–4093)** — Specifies VLAN ID associated with this group.
- **Interface** — Selects the interface(s) to add or remove from this group. Highlight the interfaces to be in the protocol group and click the right arrow. Interfaces displayed in right-hand column are part of the protocol group.
- **Remove Protocol Group** — Removes the protocol group displayed on screen when checked and **Apply Changes** is clicked. To remove multiple groups at the same time, click **Show All** and use the **Remove** check boxes on the **Protocol Group Table.**

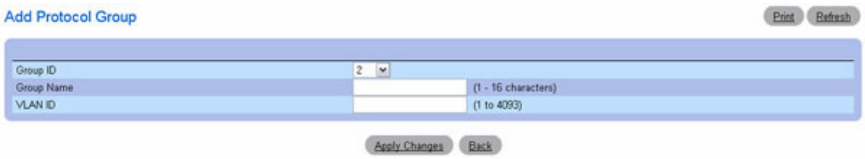
Adding a Protocol Group

1. Open the **Protocol Group** page.
2. Click **Add**.

   The **Add Protocol Group** page displays.

Downloaded from www.Manualslib.com manuals search engine

Figure 7-63. Add Protocol Group



3. Enter a new Protocol Group Name and a VLAN ID to associate with this group.
4. Return to the Protocol Group page.
5. Select the Protocol Group that you added, then select the protocol.
6. In the first Interface column, click to highlight the interfaces to be added to the protocol group. (To select multiple interfaces, press <Shift> (to select contiguous interfaces) or <Ctrl> (non-contiguous interfaces) when clicking.)
7. Click the right arrow.

   Selected interfaces move to the second column. All interfaces in this column are part of the protocol group.
8. Click **Apply Changes**.

   The protocol group is added, and the device is updated.

Modifying VLAN Protocol Group Settings

1. Open the **Protocol Group** page.
2. Specify the protocol to be modified from the Protocol Group ID drop-down menu.
3. Change Protocol or VLAN ID as needed.
4. To add an Interface to the group, click to highlight the desired interface in the first column. (To select multiple interfaces, press <Shift> (to select contiguous interfaces) or <Ctrl> (non-contiguous interfaces) when clicking.)
5. Click the right arrow.

   Selected interface moves to the second column. All interfaces in this column are part of the protocol group.
6. To remove an Interface from the group, click to highlight the desired interface in the second column.
7. Click the left arrow.

   Selected interface is removed from the second column.
8. Click **Apply Changes**.

   The VLAN protocol group parameters are modified, and the device is updated.

Downloaded from www.Manualslib.com manuals search engine

Removing Multiple Protocols From the Protocol Group Table

1. Open the **Protocol Group** page.
2. Click **Show All**.

   The **Protocol Group Table** displays.

Figure 7-64. Protocol Group Table

3. Check **Remove** for the protocol groups you want to remove.
4. Click **Apply Changes**.

   The protocol is removed, and the device is updated.

Configuring Protocol Groups Using CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- VLAN Commands

GVRP Parameters

The GARP VLAN Registration Protocol provides a mechanism that allows networking switches to dynamically register (and de-register) VLAN membership information with the MAC networking switches attached to the same segment, and for that information to be disseminated across all networking switches in the bridged LAN that support GVRP.

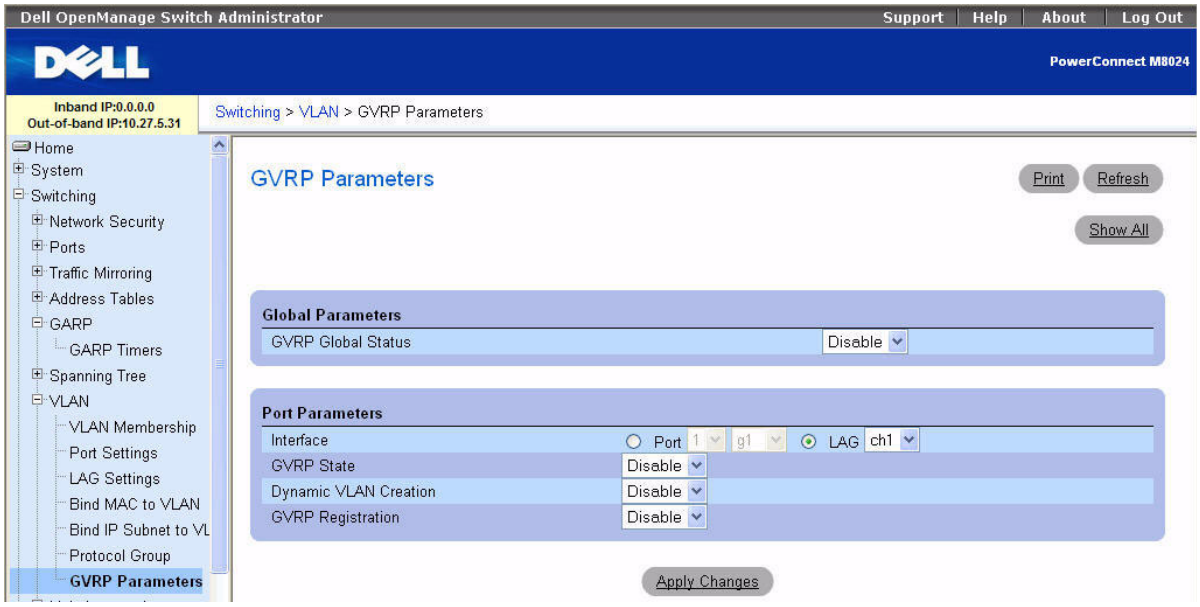
The operation of GVRP relies upon the services provided by the Generic Attribute Registration Protocol (GARP). GVRP can create up to 1024 VLANs.

Use the **GVRP Global Parameters** page to enable GVRP globally. You can also enable GVRP on a per-interface basis.

To display the **GVRP Global Parameters** page, click **Switching > VLAN > GVRP Parameters** in the tree view.

Downloaded from www.Manualslib.com manuals search engine

Figure 7-65. GVRP Global Parameters



The **GVRP Global Parameters** page contains the following fields:

- **GVRP Global Status** — Enables or disables GVRP on the switch. GVRP is disabled by default.
- **Interface** — Specifies the Unit and Port or LAG for which GVRP is enabled.
- **GVRP State** — Enables or disables GVRP on the specified interface.
- **Dynamic VLAN Creation** — Enables or disables VLAN creation through GVRP.
- **GVRP Registration** — Enables or disables GVRP Registration.

Enabling GVRP On the Switch

1. Open the **GVRP Global Parameters** page.
2. Select **Enable** in the **GVRP Global Status** field.
3. Click **Apply Changes**.

   GVRP is enabled on the switch.

Enabling VLAN Registration Through GVRP

1. Open the **GVRP Global Parameters** page.
2. Select **Enable** in the **GVRP Global Status** field for the desired interface.
3. Select **Enable** in the **GVRP Registration** field.
4. Click **Apply Changes**.

   GVRP VLAN Registration is enabled on the port, and the device is updated.

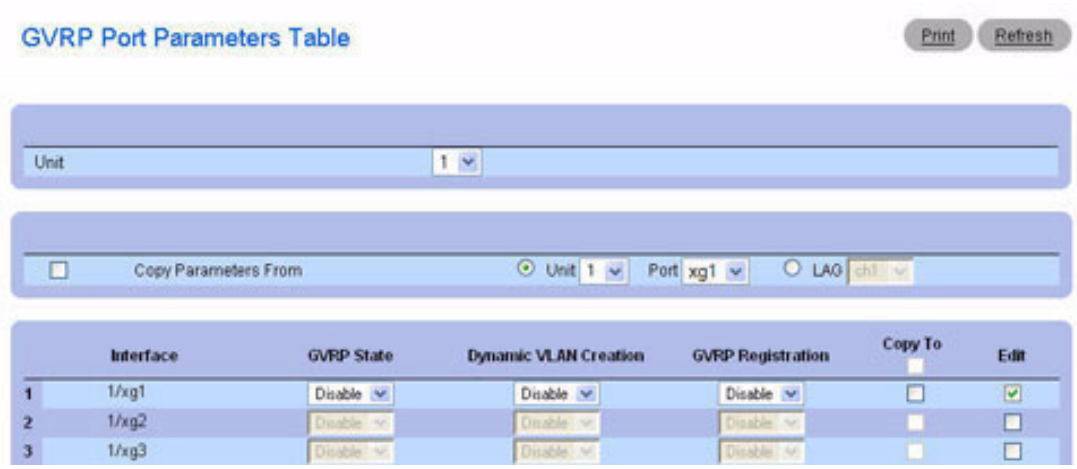
Downloaded from www.Manualslib.com manuals search engine

Displaying the GVRP Port Parameters Table

1. Open the **GVRP Global Parameters** page.
2. Click **Show All**.

   The **GVRP Port Parameters Table** displays.

Figure 7-66. GVRP Port Parameters Table



3. Use the **Unit** drop-down menu to view the **GVRP Port Parameters Table** for other units in the stack, if they exist.

Copying GVRP Parameters

1. Open the **GVRP Global Parameters** page.
2. Click **Show All**.

   The **GVRP Port Parameters Table** displays.
3. Specify the Port or LAG you are copying from in **Copy Parameters From**.
4. Click **Copy To** for each Interface/LAG to receive these parameters.
5. Click **Apply Changes**.

   The GVRP Port Parameter settings are copied, and the device is updated.

Downloaded from www.Manualslib.com manuals search engine

Modifying GVRP Parameters for Multiple Ports

1. Open the **GVRP Global Parameters** page.
2. Click **Show All**.

   The **GVRP Port Parameters Table** displays.
3. Click **Edit** for each Interface/LAG to modify.
4. Edit the GVRP Port Parameter fields as needed.
5. Click **Apply Changes**.

   The GVRP Port Parameter settings are modified, and the device is updated.

Configuring GVRP Using CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- GVRP Commands

Configuring Voice VLAN

The Voice VLAN feature enables switch ports to carry voice traffic with defined priority. The priority level enables the separation of voice and data traffic coming onto the port. A primary benefit of using Voice VLAN is to ensure that the sound quality of an IP phone is safeguarded from deteriorating when the data traffic on the port is high. The system uses the source MAC address of the traffic traveling through the port to identify the IP phone data flow.

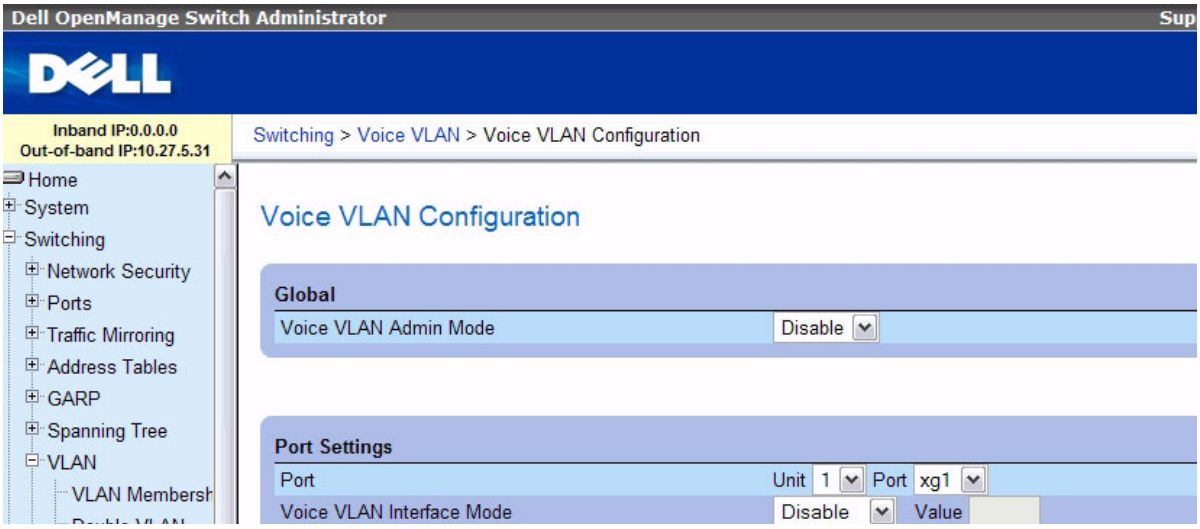
The Voice VLAN feature supports a configurable voice VLAN DSCP parameter. This allows you to set the DSCP value. This value is later retrieved by LLDP when the LLDPDU is transmitted if LLDP has been enabled on the port and the required TLV is configured for the port.

Use the **Voice VLAN Configuration** page to configure and view voice VLAN settings that apply to the entire system and to specific interfaces.

To display the page, click **Switching > Voice VLAN > Configuration** in the tree view.

Downloaded from www.Manualslib.com manuals search engine

Figure 7-67. Voice VLAN Configuration



The **Voice VLAN Configuration** page contains the following fields:

- **Voice VLAN Admin Mode** — Select the administrative mode for Voice VLAN for the switch from the drop-down menu. The default is disable.
- **Port** — Select the interface to view or configure.
- **Voice VLAN Interface Mode** —Select the Voice VLAN mode for selected interface. The default is disable. The mode can be one of the following:
  - **Disable** — Disable voice VLAN on the port.
  - **None** — Allow the IP phone to use its own configuration to send untagged voice traffic.
  - **VLAN ID** — Configure VLAN tagging for the voice traffic. The VLAN ID range is 1–4093.
  - **dot1p** — Configure Voice VLAN 802.1p priority tagging for voice traffic. The priority tag range is 0–7.
  - **Untagged** — Configure the phone to send untagged voice traffic.
- **DSCP Value** — Configures the Voice VLAN DSCP value for the port. The default value is 46.
- **CoS Override Mode** — Select the Cos Override mode for selected interface. The default is disable.
- **Operational State** — This is the operational status of the voice VLAN on the given interface.
- **Authentication Mode** — Enable or disable 802.1X authentication on the voice VLAN. When voice VLAN authentication is disabled, VoIP devices may use the voice VLAN without authenticating.

NOTE: IEEE 802.1X must be enabled on the switch before you disable voice VLAN authentication. Voice VLAN authentication can be disabled in order to allow VoIP phones that do not support authentication to send and receive unauthenticated traffic on the Voice VLAN.

Downloaded from www.Manualslib.com manuals search engine

Configuring Voice VLAN Settings

1. Open the **Voice VLAN Configuration** page.
2. Configure the settings for the system or for each port.
3. Click **Apply Changes**.

   The system parameters are applied, and the device is updated.

Configuring Voice VLAN Using CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the CLI Reference Guide:

Voice VLAN Commands

Aggregating Ports

Link Aggregation allows one or more full duplex (FDX) Ethernet links to be aggregated together to form a Link Aggregation Group (LAG). This allows the networking switch to treat the LAG as if it is a single link.

Static LAGs are supported. When a port is added to a LAG as a static member, it neither transmits nor receives LACPDUs.

To display the **Link Aggregation** menu page, click **Switching > Link Aggregation** in the tree view. The **Link Aggregation** page contains links to the following features:

- LACP Parameters
- LAG Membership
- LAG Hash Configuration
- LAG Hash Summary

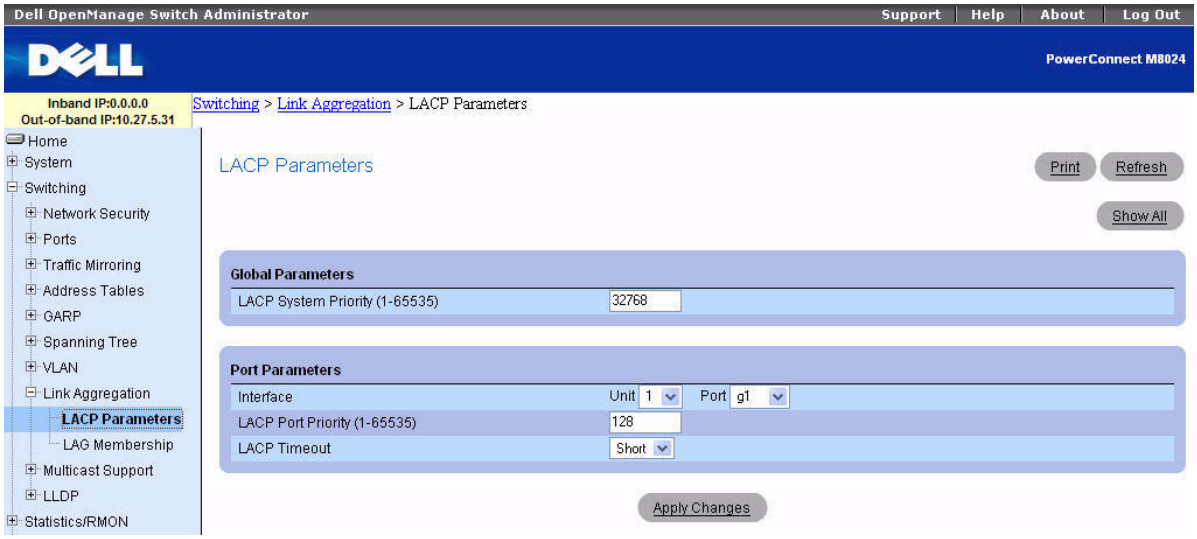
LACP Parameters

Link Aggregation is initiated and maintained by the periodic exchanges of LACPDUs. Use the **LACP Parameters** page to configure LACP LAGs.

To display the **LACP Parameters** page, click **Switching > Link Aggregation > LACP Parameters** in the tree view.

Downloaded from www.Manualslib.com manuals search engine

Figure 7-68. LACP Parameters



The **LACP Parameters** page is divided into two sections: Global Parameters and Port Parameters. Following are the fields on this page:

Global Parameters

- **LACP System Priority (1–65535)** — Indicates the LACP priority value for global settings. The default value is 1.

Port Parameters

- **Interface**— Specifies the unit and port number to which timeout and priority values are assigned.
- **LACP Port Priority (1–65535)** — Specifies LACP priority value for the specified port. The default value is 1.
- **LACP Timeout** — Specifies Administrative LACP timeout. Possible values are:
  - **Short** — Specifies a short timeout value.
  - **Long** — Specifies a long timeout value. This is the default.

Defining Link Aggregation Parameters

1. Open the **LACP Parameters** page.
2. Complete the fields as needed.
3. Click **Apply Changes**.

   The parameters are defined, and the device is updated.

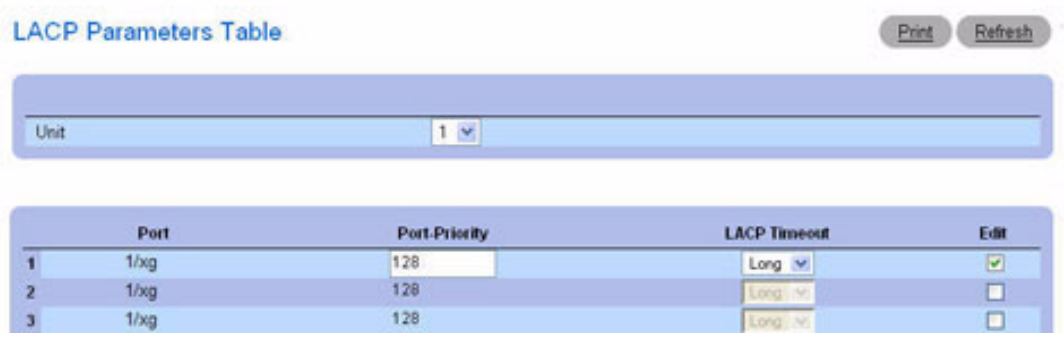
Downloaded from www.Manualslib.com manuals search engine

Displaying the LACP Parameters Table

1. Open the **LACP Parameters** page.
2. Click **Show All**.

   The **LACP Parameters Table** displays.

Figure 7-69. LACP Parameters Table



3. Use the **Unit** drop-down menu to view the **LACP Parameters Table** for other units in the stack, if they exist.

Modifying LACP Parameters for Multiple Ports

1. Open the **LACP Parameters** page.
2. Click **Show All**.

   The **LACP Parameters Table** displays.
3. Click **Edit** for each Port to modify.
4. Edit the fields as needed.
5. Click **Apply Changes**.

   The LACP Parameter settings are modified, and the device is updated.

Configuring LACP Parameters Using CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- LACP Commands

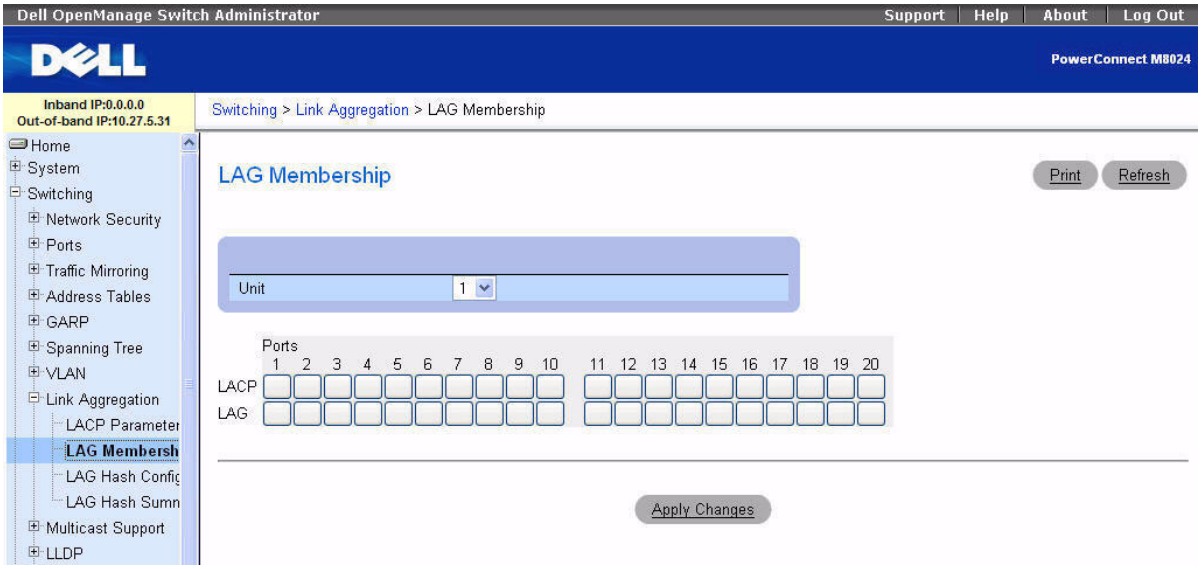
LAG Membership

Your switch supports 48 LAGs per system, and eight ports per LAG. Use the **LAG Membership** page to assign ports to LAGs and LACPs.

Downloaded from www.Manualslib.com manuals search engine

To display the **LAG Membership** page, click **Switching > Link Aggregation > LAG Membership** in the tree view.

Figure 7-70. LAG Membership



The **LAG Membership** page contains a table with the following fields:

- **LACP** — Aggregates a LAG port to LACP membership. For ports with a number in the LAG row, you can click in the **LACP** row to toggle LACP "on." Each click toggles between L (LACP) and blank (no LACP).
- **LAG** — Adds a port to a LAG, and indicates the specific LAG to which the port belongs. Each click toggles through the LAG numbers, 1–48, and then back to blank (no LAG assigned).

Adding a Port to a LAG

1. Open the **LAG Membership** page.
2. Click in the **LAG** row to toggle the port to the desired LAG.

   The LAG number displays for that port. The LAG number increases each time you click until the number reaches 48 and then returns to blank (no LAG assigned).
3. Click **Apply Changes**.

   The port is assigned to the selected LAG, and the device is updated.

Downloaded from www.Manualslib.com manuals search engine

Adding a LAG Port to an LACP

1. Open the **LAG Membership** page.
2. Click in the **LACP** row to toggle the desired LAG port to **L**.

   Note: The port must be assigned to a LAG before it can be aggregated to an LACP.
3. Click **Apply Changes**.

   The LAG port is aggregated to the LACP, and the device is updated.

Assigning Ports to LAGs and LACPs Using CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

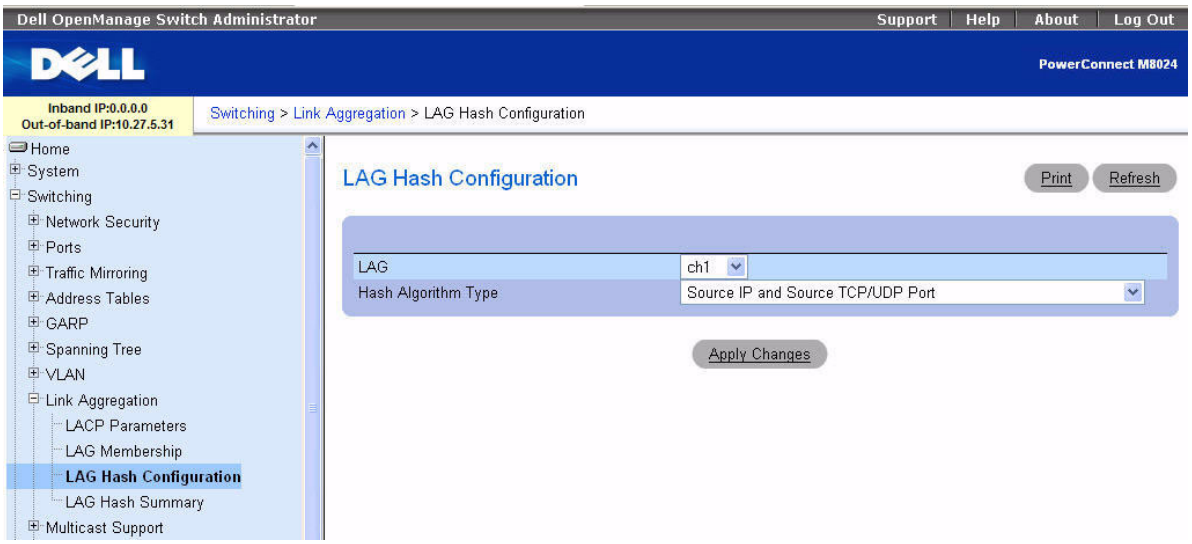
- Port Channel Commands

LAG Hash Configuration

Use the LAG HASH algorithm to set the traffic distribution mode on the aggregator link. You can set the HASH type for each trunk.

To display the **LAG Hash Configuration** page, click **Switching > Link Aggregation > LAG Hash Configuration** in the tree view.

Figure 7-71. LAG Hash Configuration



The **LAG Hash Configuration** page contains the following fields:

- **LAG** — The drop-down menu lists the LAG numbers.
- **Hash Algorithm Type** — The HASH algorithm for unicast traffic flows can be one of the following types:

Downloaded from www.Manualslib.com manuals search engine

- Source MAC, VLAN, EtherType, SourceModule and Port Id
- Destination MAC, VLAN, EtherType, SourceModule and Port Id
- Source IP and Source TCP/UDP Port (default)
- Destination IP and Destination TCP/UDP Port
- Source/Destination MAC, VLAN, EtherType, source MODID/port
- Source/Destination IP and source/destination TCP/UDP port

Configuring the LAG Hash

1. Open the **LAG Hash Configuration** page.
2. Select the LAG to configure and the hash algorithm to assign to the LAG.
3. Click **Apply Changes**.

   The parameters are modified, and the device is updated.

Configuring the LAG Hash Using CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- Port Channel Commands

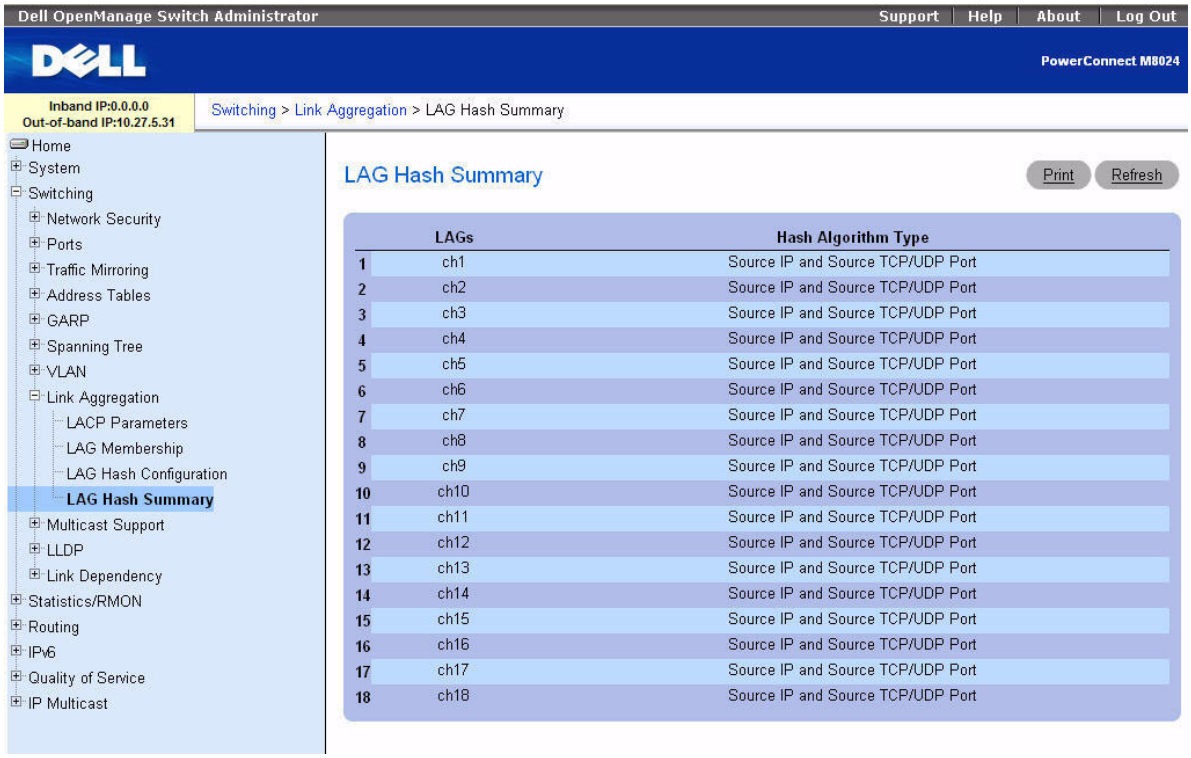
LAG Hash Summary

The **LAG Hash Summary** page lists the channels on the system and their assigned hash algorithm type.

To display the **LAG Hash Summary** page, click **Switching > Link Aggregation > LAG Hash Summary** in the tree view.

Downloaded from www.Manualslib.com manuals search engine

Figure 7-72. LAG Hash Summary



	LAGs	Hash Algorithm Type
1	ch1	Source IP and Source TCP/UDP Port
2	ch2	Source IP and Source TCP/UDP Port
3	ch3	Source IP and Source TCP/UDP Port
4	ch4	Source IP and Source TCP/UDP Port
5	ch5	Source IP and Source TCP/UDP Port
6	ch6	Source IP and Source TCP/UDP Port
7	ch7	Source IP and Source TCP/UDP Port
8	ch8	Source IP and Source TCP/UDP Port
9	ch9	Source IP and Source TCP/UDP Port
10	ch10	Source IP and Source TCP/UDP Port
11	ch11	Source IP and Source TCP/UDP Port
12	ch12	Source IP and Source TCP/UDP Port
13	ch13	Source IP and Source TCP/UDP Port
14	ch14	Source IP and Source TCP/UDP Port
15	ch15	Source IP and Source TCP/UDP Port
16	ch16	Source IP and Source TCP/UDP Port
17	ch17	Source IP and Source TCP/UDP Port
18	ch18	Source IP and Source TCP/UDP Port

The **LAG Hash Summary** page contains a table with the following fields:

- **LAGs** — Lists the LAG numbers.
- **Hash Algorithm Type** — Shows the type of HASH algorithm for unicast traffic flows that is associated with the LAG.

Viewing the LAG Hash Algorithm Summary Using CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- Port Channel Commands

Managing Multicast Support

The Layer 2 Multicast Forwarding Database is used by the switch to make forwarding decisions for packets that arrive with a multicast destination MAC address. By limiting multicasts to only certain ports in the switch, traffic is prevented from going to parts of the network where that traffic is unnecessary.

When a packet enters the switch, the destination MAC address is combined with the VLAN ID and a search is performed in the Layer 2 Forwarding database. If no match is found, then the packet is either flooded to all ports in the VLAN or discarded, depending on the switch configuration. If a match is found, then the packet is forwarded only to the ports that are members of that multicast group.

Downloaded from www.Manualslib.com manuals search engine

To display the **Multicast Support** menu page, click **Switching > Multicast Support** in the tree view. This **Multicast Support** page contains links to the following features:

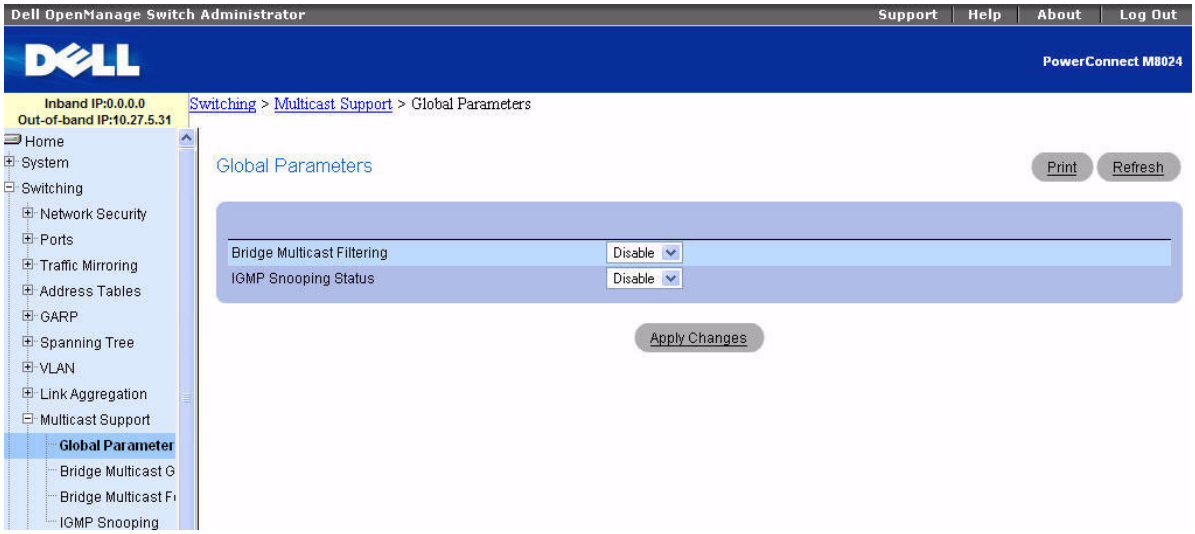
- Multicast Global Parameters
- Bridge Multicast Group
- Bridge Multicast Forward
- IGMP Snooping
- MRouter Status
- MLD Snooping

Multicast Global Parameters

Use the **Multicast Global Parameters** page to enable bridge multicast filtering or IGMP Snooping on the switch. Parameters for these features can be modified from the **Bridge Multicast Forward** and **IGMP Snooping** web pages.

To display the **Multicast Global Parameters** page, click **Switching > Multicast Support > Global Parameters** in the tree view.

Figure 7-73. Multicast Global Parameters



The **Multicast Global Parameters** page contains the following field:

- **Bridge Multicast Filtering** — Enables or disables bridge Multicast filtering. The default value is disabled.
- **IGMP Snooping Status** — Enables or disables IGMP snooping. The default value is disabled.

Downloaded from www.Manualslib.com manuals search engine

Enabling Bridge Multicast Filtering on the Switch

1. Open the **Multicast Global Parameters** page.
2. Select **Enable** in the **Bridge Multicast Filtering** field.
3. Click **Apply Changes**.

   Bridge Multicast is enabled on the switch.

Enabling Multicast Forwarding and/or IGMP Snooping Using CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- Address Table Commands

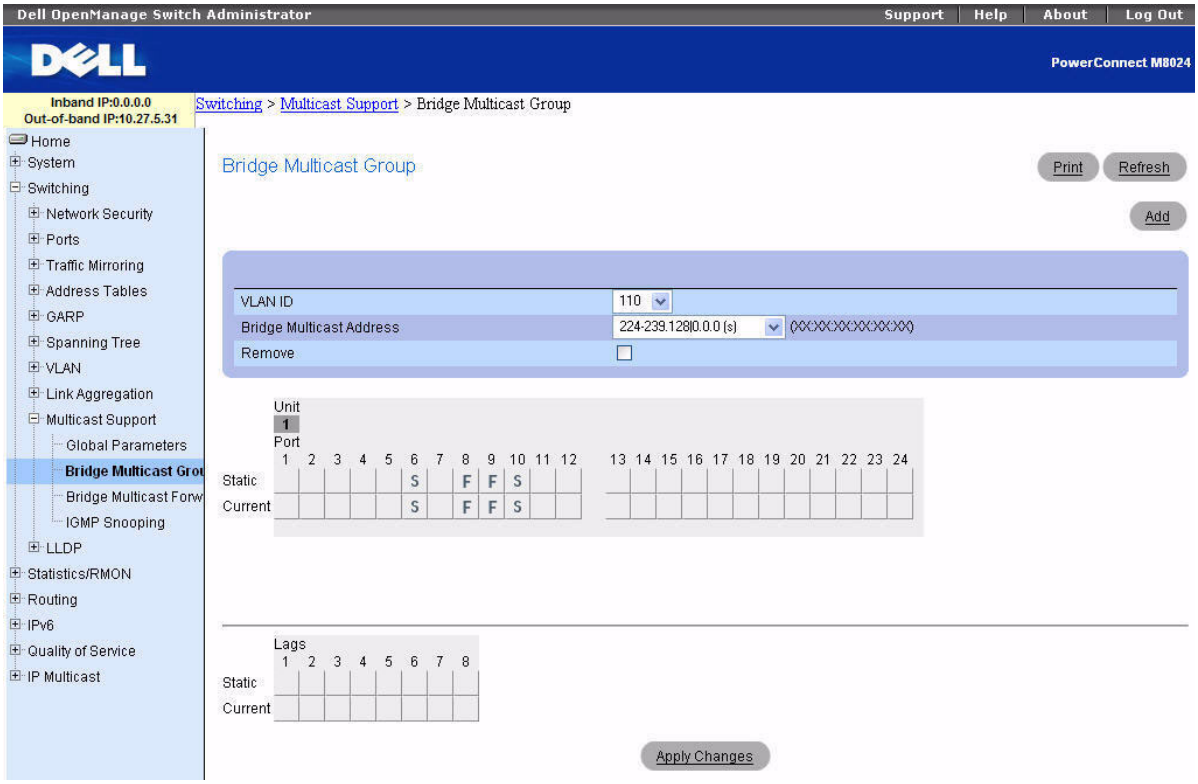
Bridge Multicast Group

Use the **Bridge Multicast Group** page to create new multicast service groups or to modify ports and LAGs assigned to existing multicast service groups. Attached interfaces display in the Port and LAG tables, and reflect the manner in which each is joined to the Multicast group.

To display the **Bridge Multicast Group** page, click **Switching > Multicast Support > Bridge Multicast Group** in the tree view.

Downloaded from www.Manualslib.com manuals search engine

Figure 7-74. Bridge Multicast Group



The **Bridge Multicast Group** page contains the following fields:

- **VLAN ID** — Selects the VLAN to add a multicast group to or to modify ports on an existing multicast group.
- **Bridge Multicast Address** — Identifies the multicast group MAC address/IP address associated with the selected VLAN ID. Use the **Add** button to associate a new address with a VLAN ID.
- **Remove** — Removes a Bridge Multicast address when checked.

Port and LAG Member Tables

The **Bridge Multicast Group** tables display which Ports and LAGs are members of the multicast group, and whether they're static (S), dynamic (D), or forbidden (F). The tables have two rows: **Static** and **Current**. Only the **Static** row is accessible from this page. The **Current** row is updated when the **Static** row is changed and **Apply Changes** is clicked.

The **Bridge Multicast Group** page contains two editable tables:

- **Unit and Ports** — Displays and assigns multicast group membership to ports. To assign membership, click in **Static** for a specific port. Each click toggles between S, F, and blank. See the following table for definitions.

Downloaded from www.Manualslib.com manuals search engine

- **LAGs** — Displays and assigns multicast group membership to LAGs. To assign membership, click in **Static** for a specific LAG. Each click toggles between S, F, and blank. See the following table for definitions.

The following table contains definitions for port/LAG IGMP management settings.

Table 7-2. Port/LAG IGMP Management Settings

Port Control	Definition
D	Dynamic: Indicates that the port/LAG was dynamically joined to the Multicast group (displays in the *Current* row).
S	Static: Attaches the port to the Multicast group as a static member in the *Static* row. Displays in the *Current* row once **Apply Changes** is clicked.
F	Forbidden: Indicates that the port/LAG is forbidden entry into the Multicast group in the *Static* row. Displays in the *Current* row once **Apply Changes** is clicked.
Blank	Blank: Indicates that the port is not attached to a Multicast group.

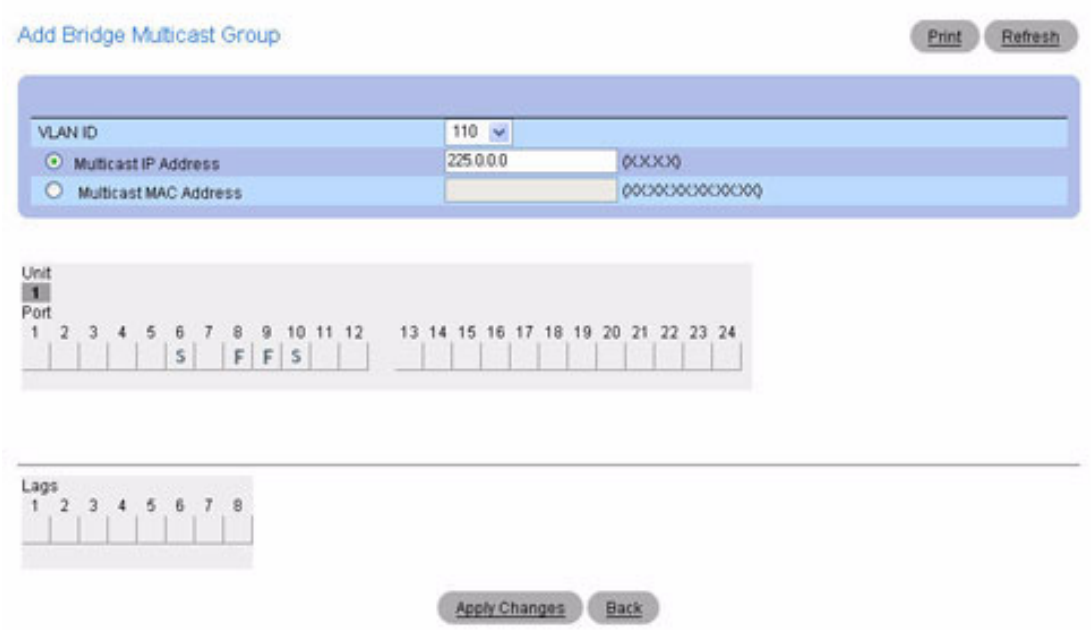
Adding Bridge Multicast Addresses

1. Open the **Bridge Multicast Group** page.
2. Click **Add**.

   The **Add Bridge Multicast Group** page displays.

Downloaded from www.Manualslib.com manuals search engine

Figure 7-75. Add Bridge Multicast Group



3. Select the **VLAN ID** from the drop-down menu.
4. Define the **New Bridge Multicast IP or MAC** address.
5. In the **Bridge Multicast Group** tables, assign a setting by clicking in the **Static** row for a specific port/LAG. Each click toggles between S, F, and blank. (not a member).
6. Click **Apply Changes**.

   The bridge multicast address is assigned to the multicast group, ports/LAGs are assigned to the group (with the **Current** rows being updated with the **Static** settings), and the device is updated.

Assigning an Interface to an existing Multicast Group

1. Open the **Bridge Multicast Group** page.
2. Select the **VLAN ID** from the drop-down menu.

   The associated **Bridge Multicast Address** displays.
3. In the **Bridge Multicast Group** tables, assign a setting by clicking in the **Static** row for a specific port/LAG. Each click toggles between S, F, and blank (not a member).
4. Click **Apply Changes**.

   The interface is assigned to the multicast group, the **Current** row is updated with the **Static** setting, and the device is updated.

Downloaded from www.Manualslib.com manuals search engine

Removing a Bridge Multicast Group

1. Open the **Bridge Multicast Group** page.
2. Select the **VLAN ID** associated with the bridge multicast group to be removed from the drop-down menu.

   The **Bridge Multicast Address** and the assigned ports/LAGs display.
3. Check the **Remove** check box.
4. Click **Apply Changes**.

   The selected bridge multicast group is removed, and the device is updated.

Managing Multicast Service Members Using CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

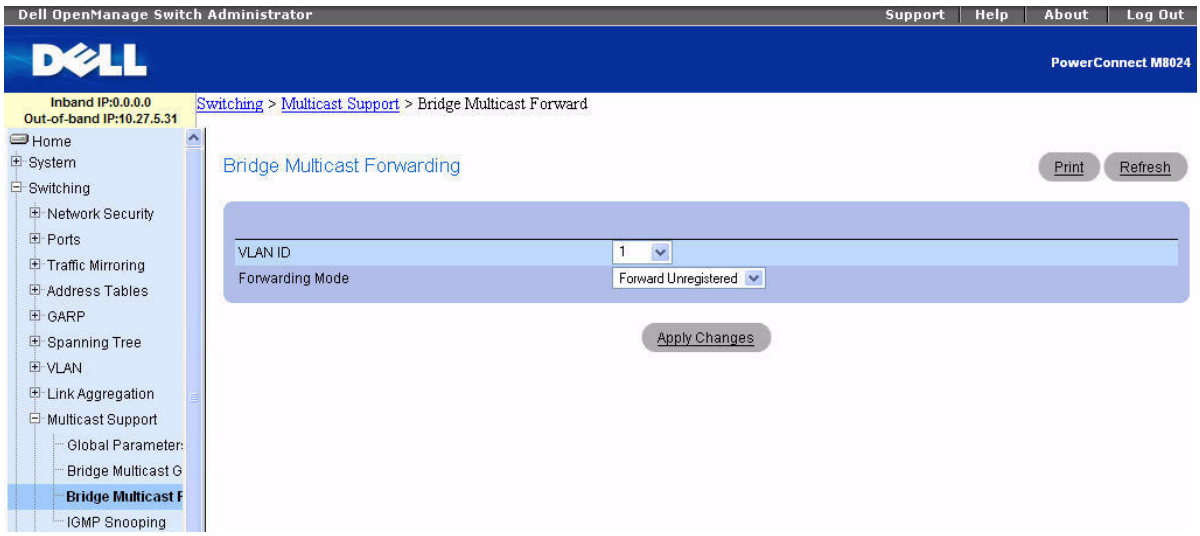
- Address Table Commands

Bridge Multicast Forward

Use the **Bridge Multicast Forward** page to enable attaching ports or LAGs to a switch that is attached to a neighboring Multicast switch. Once IGMP Snooping is enabled, multicast packets are forwarded to the appropriate port or VLAN.

To display the **Bridge Multicast Forward** page, click **Switching > Multicast Support > Bridge Multicast Forward** in the tree view.

Figure 7-76. Bridge Multicast Forward



The **Bridge Multicast Forward** page contains the following field and two editable tables:

- **VLAN ID** — Selects the VLAN to be affected.

Downloaded from www.Manualslib.com manuals search engine

- **Forwarding Mode** — Specifies the multicast forwarding mode for the selected VLAN. Possible values are:
  - **Forward Unregistered** — Permits the forwarding of IPv4 multicast packets with a destination address that does not match any of the groups announced in earlier IGMP Membership Reports.
  - **Forward All** — Permits registered and unregistered multicast packets to forward.
  - **Filter Unregistered** — Prohibits the forwarding of IPv4 multicast packets with a destination address that does not match any of the groups announced in earlier IGMP Membership Reports.

Changing the Bridge Multicast Forwarding Mode.

1. Open the **Bridge Multicast Forward** page.
2. Select the **VLAN ID** from the drop-down menu.
3. Select the **Forwarding Mode** to assign the VLAN from the drop-down menu.
4. Click **Apply Changes**.

   The VLAN is updated with the **Forwarding Mode** setting, and the device is updated.

Managing LAGs and Ports Attached to Multicast Routers Using CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- Address Table Commands

IGMP Snooping

Internet Group Management Protocol (IGMP) Snooping is a feature that allows a switch to forward multicast traffic intelligently on the switch. Multicast IP traffic is traffic that is destined to a host group. Host groups are identified by class D IP addresses, which range from 224.0.0.0 to 239.255.255.255. Based on the IGMP query and report messages, the switch forwards traffic only to the ports that request the multicast traffic. This prevents the switch from broadcasting the traffic to all ports and possibly affecting network performance.

When a packet with a broadcast or multicast destination address is received, the switch will forward a copy into each of the remaining network segments in accordance with the IEEE MAC Bridge standard. Eventually, the packet is made accessible to all nodes connected to the network.

This approach works well for broadcast packets that are intended to be seen or processed by all connected nodes. In the case of multicast packets, however, this approach could lead to less efficient use of network bandwidth, particularly when the packet is intended for only a small number of nodes. Packets will be flooded into network segments where no node has any interest in receiving the packet.

Allowing switches to snoop IGMP packets is a creative effort to solve this problem. The switch uses the information in the IGMP packets as they are being forwarded throughout the network to determine which segments should receive packets directed to the group address.

Downloaded from www.Manualslib.com manuals search engine

To display the **IGMP Snooping** page, click **Switching** > **Multicast Support** > **IGMP Snooping** in the tree view. Use this page to go to the following features:

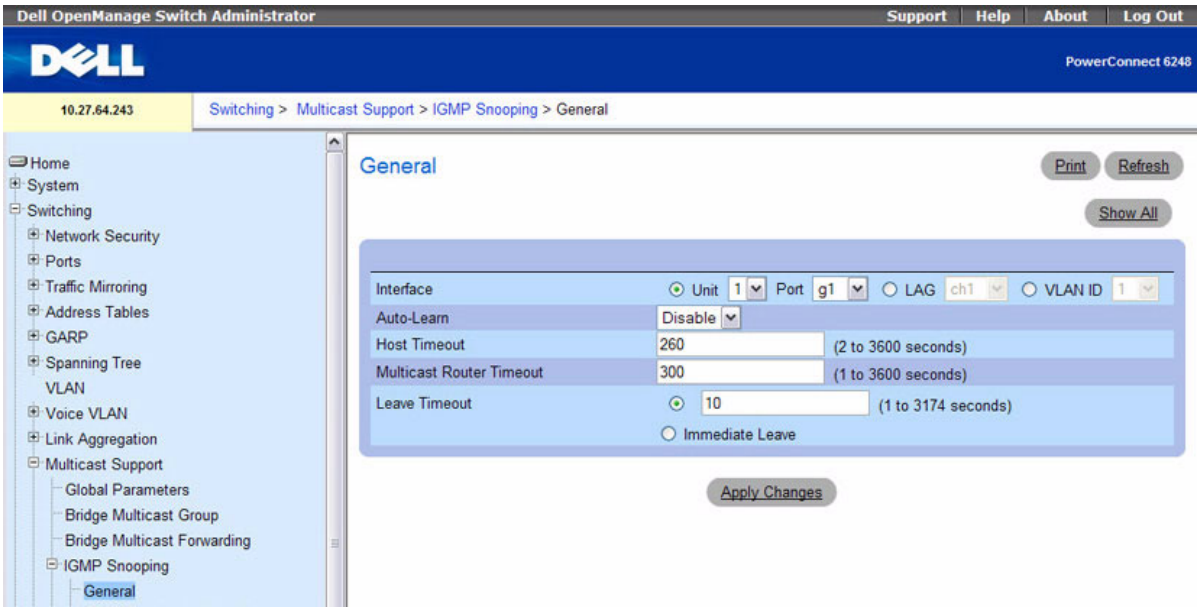
- General IGMP Snooping
- Global Querier Configuration
- VLAN Querier
- VLAN Querier Status
- MFDB IGMP Snooping Table

General IGMP Snooping

Use the **General** IGMP snooping page to add IGMP members.

To display the **General** IGMP snooping page, click **Switching** > **Multicast Support** > **IGMP Snooping** > **General** in the tree view.

Figure 7-77. General IGMP Snooping



The **General** IGMP snooping page contains the following fields:

- **Interface —** Selects the Unit and Port, LAG, or VLAN to be affected.
- **Auto-Learn** — Enables or disables Auto-Learn on the switch.
- **Host Timeout** — Specifies time before an IGMP snooping entry is aged out. The default time is 260 seconds.

Downloaded from www.Manualslib.com manuals search engine

- **Multicast Router Timeout** — Specifies time before aging out a Multicast router entry. The default value is 300 seconds.
- **Leave Timeout** — Specifies time, in seconds, after a port leave message is received before the entry is aged out. Enter an amount of time for the timeout period, or click **Immediate Leave** to specify an immediate timeout. The default timeout is 10 seconds.

Enabling IGMP Snooping on an Interface

1. Open the **General** IGMP snooping page.
2. Select the unit and port, LAG, or VLAN to configure from the **Interface** field.
3. Complete the fields on the page as needed.
4. Click **Apply Changes**.

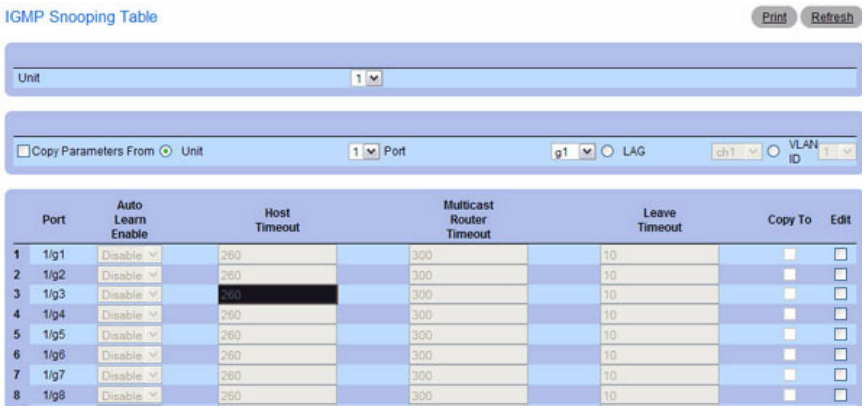
   IGMP snooping is enabled on the selected interface.

Displaying the IGMP Snooping Table

1. Open the **IGMP Snooping** page.
2. Click **Show All**.

   The **IGMP Snooping Table** displays.

Figure 7-78. IGMP Snooping Table



3. Use the **Unit** drop-down menu to view the **IGMP Snooping Table** for other units in the stack, if they exist.

Downloaded from www.Manualslib.com manuals search engine

Modifying IGMP Snooping Settings for Multiple Ports, LAGs, or VLANs

1. Open the **General** IGMP snooping page.
2. Click **Show All**.

   The **IGMP Snooping Table** displays.
3. Click **Edit** for each Port, LAG, or VLAN to modify.
4. Edit the IGMP Snooping fields as needed.
5. Click **Apply Changes**.

   The IGMP Snooping settings are modified, and the device is updated.

Copying IGMP Snooping Settings to Multiple Ports, LAGs, or VLANs

1. Open the **General** IGMP snooping page.
2. Click **Show All**.

   The **IGMP Snooping Table** displays.
3. Click **Copy Parameters From**.
4. Select a Unit/Port, LAG, or VLAN to use as the source of the desired parameters.
5. Click **Copy To** for the Unit/Ports, LAGs, or VLANs that these parameters will be copied to.
6. Click **Apply Changes**.

   The IGMP Snooping settings are modified, and the device is updated.

Configuring General IGMP Snooping Settings with CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the CLI Reference Guide:

- IGMP Snooping Commands

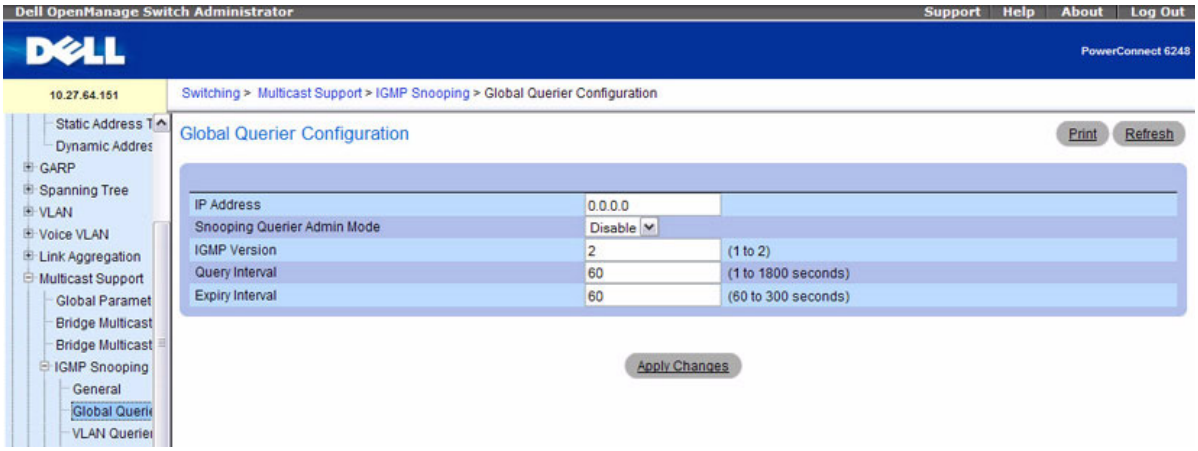
Global Querier Configuration

Use the **Global Querier Configuration** page to configure the parameters for the IGMP Snooping Querier.

To display the **Global Querier Configuration** page, click **Switching > Multicast Support > IGMP Snooping > Global Querier Configuration** in the tree view.

Downloaded from www.Manualslib.com manuals search engine

Figure 7-79. Global Querier Configuration



The **Global Querier Configuration** page contains the following fields:

- **IP Address—** Specifies the Snooping Querier IP Address which will be used as the source address in periodic IGMP queries. This address is used when no address is configured for the VLAN on which the query is being sent.
- **Snooping Querier Admin Mode** — Enables or disables the administrative mode for IGMP Snooping for the switch.
- **IGMP Version** — Specifies the version of IGMP protocol used in periodic IGMP queries.
- **Query Interval (1–1800)** — Specifies the time interval in seconds between periodic queries sent by the Snooping Querier. The default value is 60.
- **Expiry Interval (60–300)** — Specifies the time interval in seconds after which the last querier information is removed. The default value is 60.

Configuring IGMP Snooping Global Querier Settings with CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the CLI Reference Guide:

- IGMP Snooping Commands

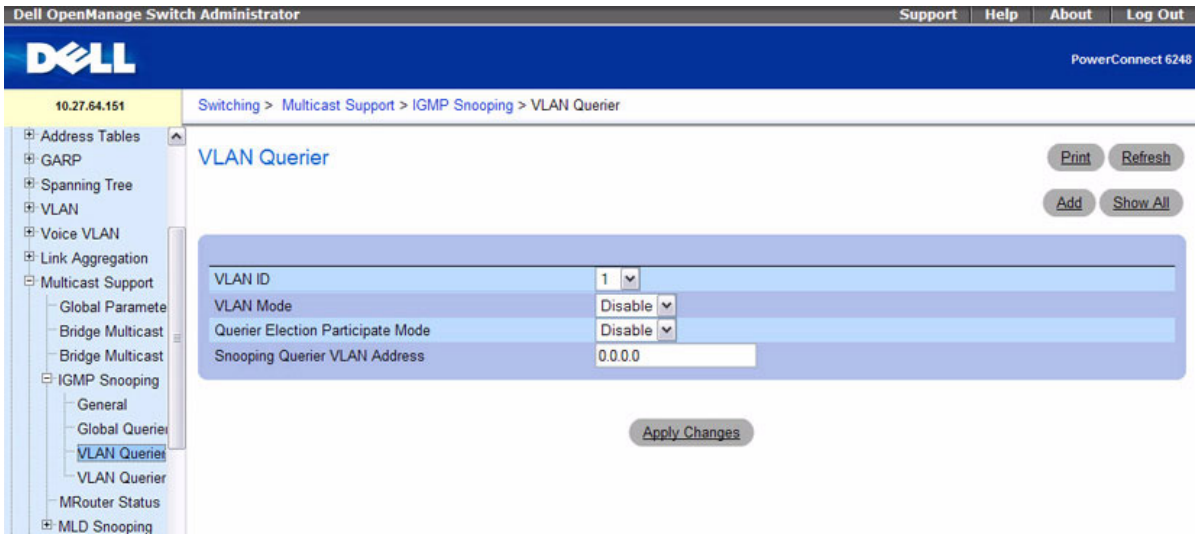
Downloaded from www.Manualslib.com manuals search engine

VLAN Querier

Use the **VLAN Querier** page to specify the IGMP Snooping Querier settings for individual VLANs.

To display the **VLAN Querier** page, click **Switching > Multicast Support > IGMP Snooping > VLAN Querier** in the tree view.

Figure 7-80. VLAN Querier



The **VLAN Querier** page contains the following fields:

- **VLAN ID** — Specifies the VLAN for the IGMP Snooping Querier configuration.
- **VLAN Mode** — Enables or disables the IGMP Snooping Querier on the VLAN selected in the VLAN ID field.
- **Querier Election Participate Mode** — Enables or disables the IGMP participation in election mode by the Snooping Querier. When this mode is disabled, upon seeing another querier of same version in the VLAN, the Snooping Querier transitions to non-querier state. When this mode is enabled, the Snooping Querier participates in querier election, where in the lowest IP address wins the querier election and operates as the querier in that VLAN. The other querier transitions to non-querier state.
- **Snooping Querier VLAN Address** — Specifies the Snooping Querier address to be used as source address in periodic IGMP queries sent on the specified VLAN.

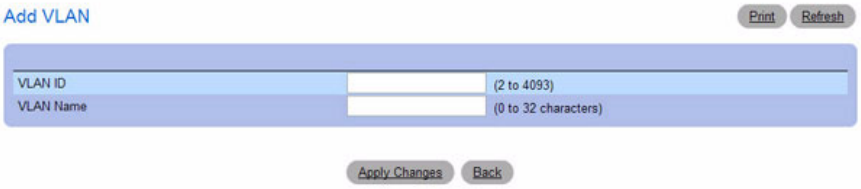
Downloaded from www.Manualslib.com manuals search engine

Adding a New VLAN and Configuring its VLAN Querier Settings

1. Open the **VLAN Querier** page.
2. Click **Add**.

   The page refreshes, and the **Add VLAN** page displays.

Figure 7-81. Add VLAN Querier



3. Enter the VLAN ID and, if desired, an optional VLAN name.
4. Complete the fields on the page as needed.
5. Click **Apply Changes**.

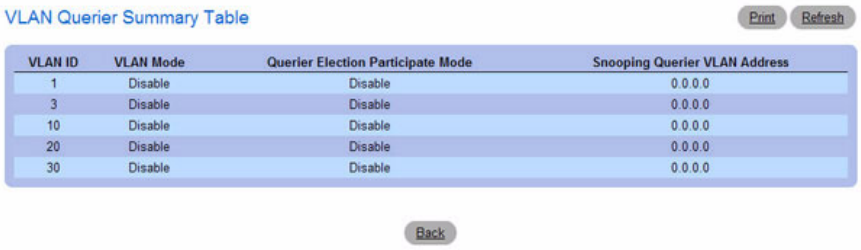
   The VLAN Querier settings are modified, and the device is updated.

Displaying the VLAN Querier Summary Table

1. Open the **VLAN Querier** page.
2. Click **Show All**.

   The **VLAN Querier Summary Table** displays.

Figure 7-82. VLAN Querier Summary Table



VLAN ID	VLAN Mode	Querier Election Participate Mode	Snooping Querier VLAN Address
1	Disable	Disable	0.0.0.0
3	Disable	Disable	0.0.0.0
10	Disable	Disable	0.0.0.0
20	Disable	Disable	0.0.0.0
30	Disable	Disable	0.0.0.0

Configuring VLAN Querier Settings with CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the CLI Reference Guide:

- IGMP Snooping Commands

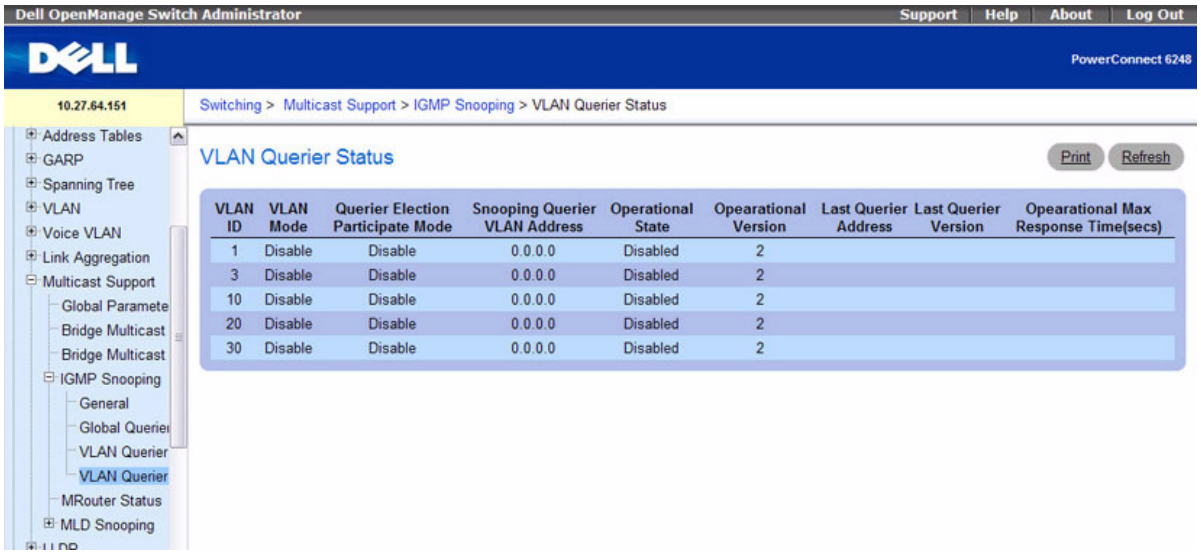
Downloaded from www.Manualslib.com manuals search engine

VLAN Querier Status

Use the **VLAN Querier Status** page to view the IGMP Snooping Querier settings for individual VLANs.

To display the **VLAN Querier Status** page, click **Switching > Multicast Support > IGMP Snooping > VLAN Querier Status** in the tree view.

Figure 7-83. IGMP Snooping VLAN Querier Status



VLAN ID	VLAN Mode	Querier Election Participate Mode	Snooping Querier VLAN Address	Operational State	Opearational Version	Last Querier Address	Last Querier Version	Opearational Max Response Time(secs)
1	Disable	Disable	0.0.0.0	Disabled	2			
3	Disable	Disable	0.0.0.0	Disabled	2			
10	Disable	Disable	0.0.0.0	Disabled	2			
20	Disable	Disable	0.0.0.0	Disabled	2			
30	Disable	Disable	0.0.0.0	Disabled	2			

The **VLAN Querier Status** page contains the following fields:

- **VLAN ID** — Identifies the VLAN.
- **VLAN Mode** — Shows whether the IGMP Snooping Querier is enabled or disabled on the VLAN.
- **Querier Election Participate Mode** — Shows whether the mode is enabled or disabled. When this mode is disabled, upon seeing another querier of same version in the VLAN, the Snooping Querier transitions to non-querier state. When this mode is enabled, the Snooping Querier participates in querier election, where in the lowest IP address wins the querier election and operates as the querier in that VLAN. The other querier transitions to non-querier state.
- **Snooping Querier VLAN Address** — Identifies the Snooping Querier address to be used as source address in periodic IGMP queries sent on the VLAN.
- **Operational State** — Displays the operational state of the IGMP Snooping Querier on the specified VLAN. It can be in any of the following states:
  - **Querier** — The Snooping switch that is the Querier in the VLAN. The Snooping switch will send out periodic queries with a time interval equal to the configured querier Query Interval. If the Snooping switch sees a better querier in the VLAN, it transitions to non-querier mode.
  - **Non-Querier** — The Snooping switch is in Non-Querier mode in the VLAN. If the querier Expiry Interval timer is expires, the Snooping switch will transition into querier mode.

Downloaded from www.Manualslib.com manuals search engine

– **Disabled** — The Snooping Querier is not operational on the VLAN. The Snooping Querier transitions to disabled mode when 1) IGMP Snooping is not operational on the VLAN, 2) the querier address is not configured or 3) the network management address is not configured.

- **Operational Version** — Displays the operational IGMP protocol version of the querier.
- **Last Querier Address** — Displays the IP address of the last querier from which a query was snooped on the VLAN.
- **Last Querier Version** — Displays the IGMP protocol version of the last querier from which a query was snooped on the VLAN.
- **Operational Max Response Time** — Displays the maximum response time to be used in the queries that are sent by the Snooping Querier.

Viewing VLAN Querier Status with CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the CLI Reference Guide:

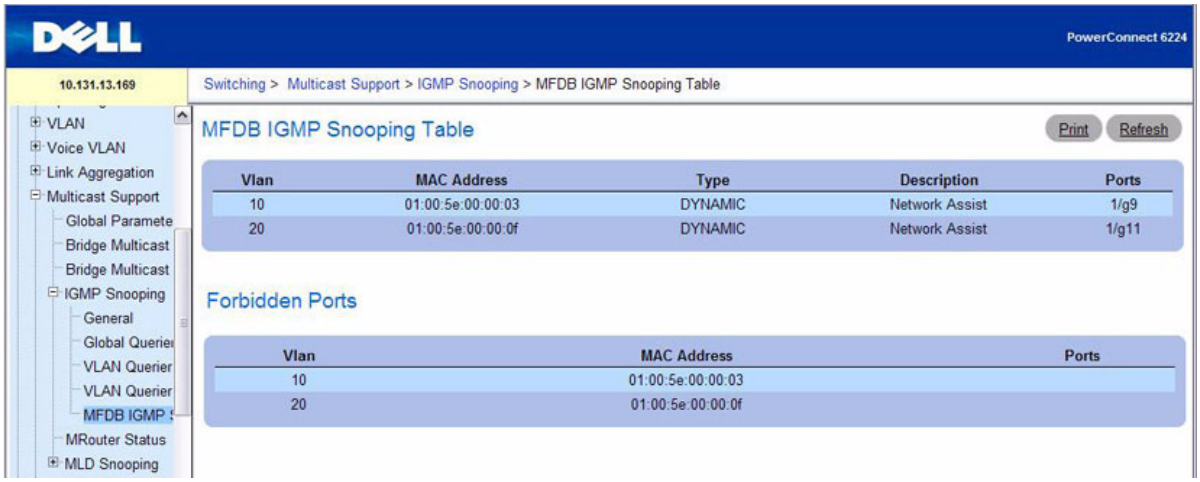
- IGMP Snooping Commands

MFDB IGMP Snooping Table

Use the **MFDB IGMP Snooping Table** page to view the MFDB IGMP Snooping Table and Forbidden Ports settings for individual VLANs.

To display the **MFDB IGMP Snooping Table** page, click **Switching > Multicast Support > IGMP Snooping > MFDB IGMP Snooping Table** in the tree view.

Figure 7-84. MFDB IGMP Snooping Table



Downloaded from www.Manualslib.com manuals search engine

The **MFDB IGMP Snooping Table** page contains the following fields:

- **VLAN** — Displays the VLAN ID associated with an IGMP group entry in the MFDB table.
- **MAC Address** — Displays the MAC Address associated with an IGMP group entry in the MFDB table.
- **Type** — Displays the type of the entry. **Static** entries are those that are configured by the user. **Dynamic** entries are added to the table as a result of a learning process or protocol.
- **Description** — The text description of this multicast table entry. Possible values are **Management Configured**, **Network Configured** and **Network Assisted**.
- **Ports** — The list of interfaces designated for forwarding (Fwd:) for a corresponding MFDB entry.

The **Forbidden Ports** section of the page contains the following fields:

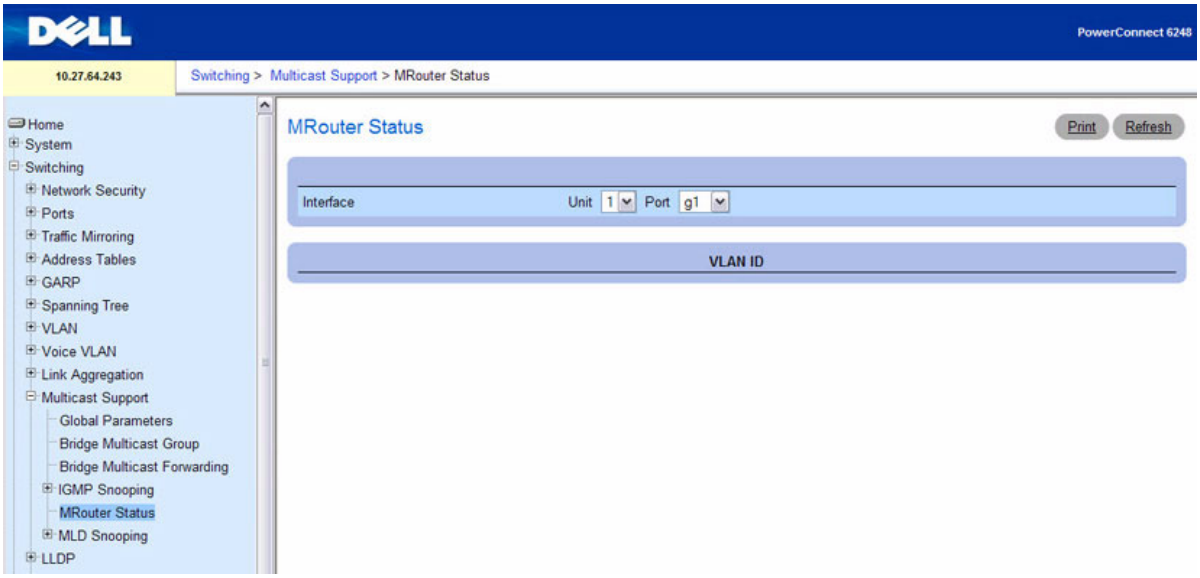
- **VLAN** — Displays the VLAN ID associated with an IGMP group entry in the MFDB table.
- **MAC Address** — Displays the MAC Address associated with an IGMP group entry in the MFDB table.
- **Ports** — The list of interfaces that are designated for filtering (Flt:) for a corresponding MFDB entry.

MRouter Status

Use the **MRouter Status** page to display the status of dynamically learned multicast router interfaces.

To access this page, click **Switching > Multicast Support > MRouter Status** in the navigation tree.

Figure 7-85. MRouter Status



The **MRouter Status** page contains the following fields:

- **Interface** — Select the interface for which you want to display the status.
- **VLAN ID —** Displays the dynamically learned multicast router interfaces.

Downloaded from www.Manualslib.com manuals search engine

MLD Snooping

In IPv4, Layer 2 switches can use IGMP snooping to limit the flooding of multicast traffic by dynamically configuring Layer-2 interfaces so that multicast traffic is forwarded to only those interfaces associated with an IP multicast address. In IPv6, MLD snooping performs a similar function. With MLD snooping, IPv6 multicast data is selectively forwarded to a list of ports that want to receive the data instead of being flooded to all ports in a VLAN. This list is constructed by snooping IPv6 multicast control packets.

MLD is a protocol used by IPv6 multicast routers to discover the presence of multicast listeners (nodes wishing to receive IPv6 multicast packets) on its directly-attached links and to discover which multicast packets are of interest to neighboring nodes. MLD is derived from IGMP; MLD version 1 (MLDv1) is equivalent to IGMPv2, and MLD version 2 (MLDv2) is equivalent to IGMPv3. MLD is a subprotocol of Internet Control Message Protocol version 6 (ICMPv6), and MLD messages are a subset of ICMPv6 messages.

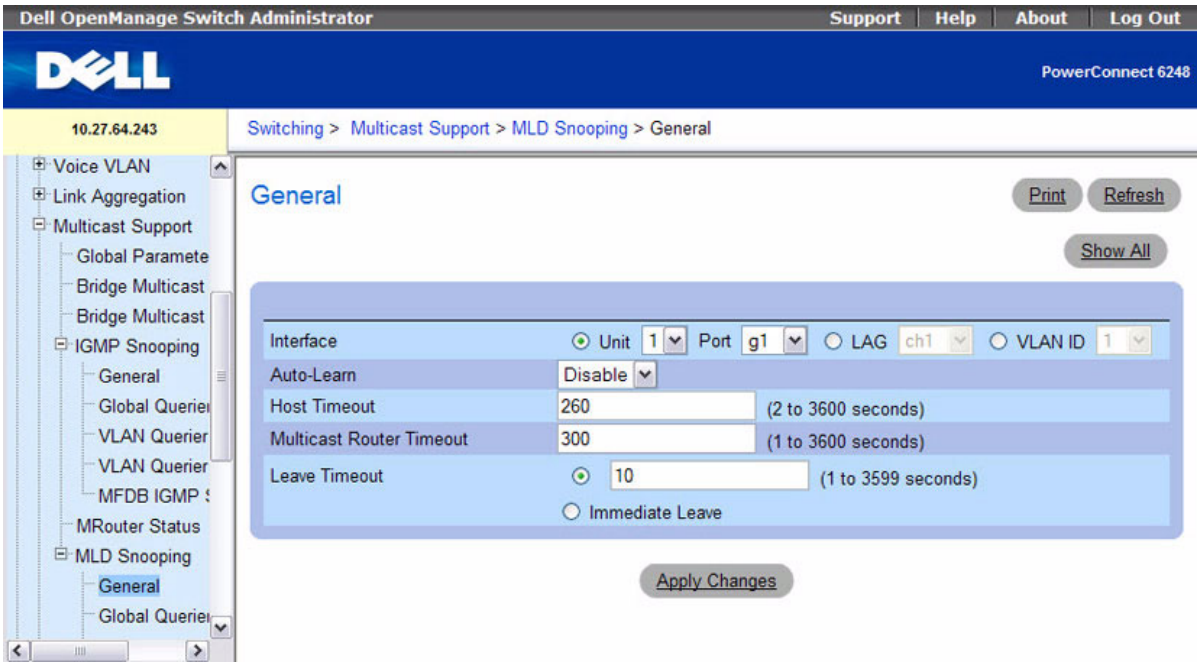
The switch can snoop on both MLDv1 and MLDv2 protocol packets and bridge IPv6 multicast data based on destination IPv6 multicast MAC addresses. The switch can be configured to perform MLD snooping and IGMP snooping simultaneously.

MLD Snooping General

Use the MLD Snooping **General** page to add MLD members.

To access this page, click **Switching > Multicast Support > MLD Snooping > General** in the navigation tree.

Figure 7-86. MLD Snooping General



Downloaded from www.Manualslib.com manuals search engine

The MLD Snooping **General** page contains the following fields:

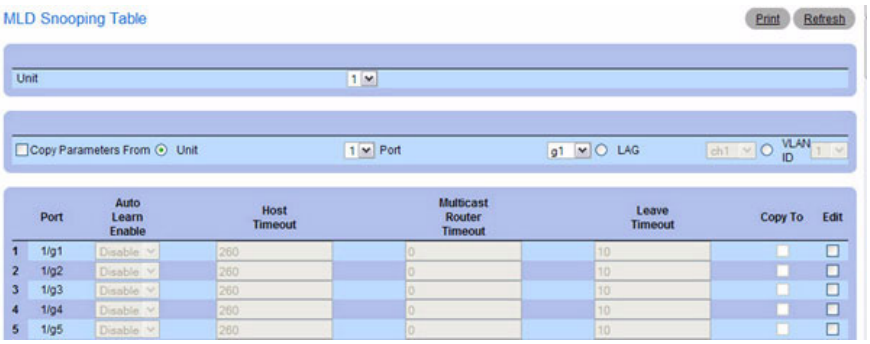
- Interface — Specifies the Unit and Port or the LAG on which MLD Snooping should be enabled.
- Auto Learn — Enable or Disable the ability of the switch to automatically learn about dynamic MLD ports.
- Host Timeout — Specifies time (in seconds) before an MLD snooping entry is aged out. The range is from 2 to 3600 seconds. The default time is 260 seconds.
- Multicast Router Timeout — Specifies time (in seconds) before aging out a Multicast router entry. The range is 1 to 3600 seconds. The default value is 300 seconds.
- Leave Timeout — Specifies the amount of time (in seconds) after a port leave message is received before the entry is aged out. Enter value for the timeout period, or click Immediate Leave to specify an immediate timeout. The range is from 1 to 3599 seconds. The default timeout is 10 seconds.

Displaying the MLD Snooping Table

1. Open the MLD Snooping **General** page.
2. Click **Show All**.

   The **MLD Snooping Table** displays.

Figure 7-87. MLD Snooping Table



Copying MLD Snooping Settings to Multiple Ports, LAGs, or VLANs

1. Open the **General** MLD snooping page.
2. Click **Show All**.

   The **MLD Snooping Table** displays.
3. Click **Copy Parameters From**.
4. Select a Unit/Port, LAG, or VLAN to use as the source of the desired parameters.
5. Click **Copy To** for the Unit/Ports, LAGs, or VLANs that these parameters will be copied to.
6. Click **Apply Changes**.

   The MLD Snooping settings are modified, and the device is updated.

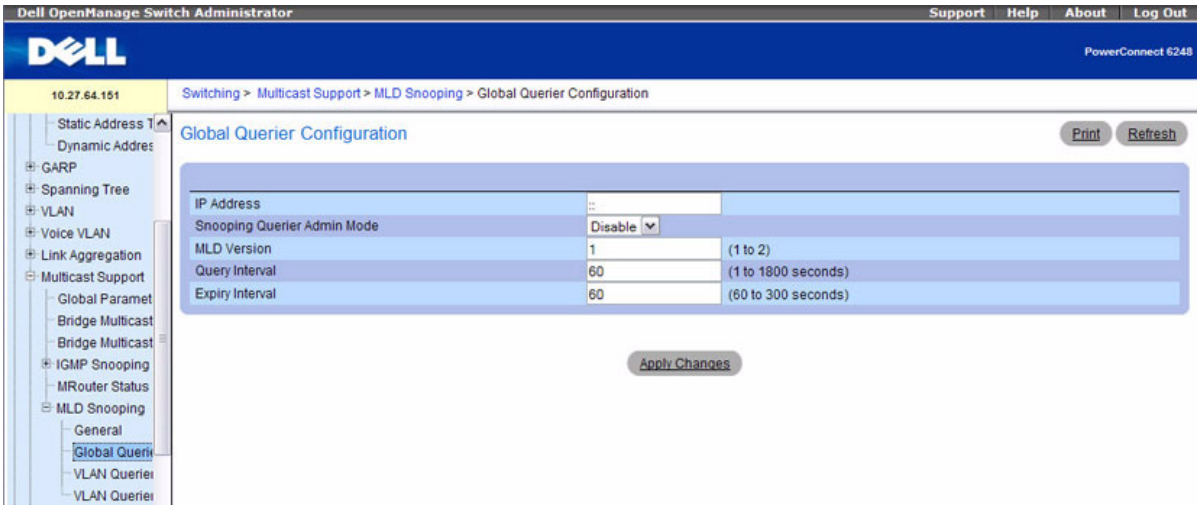
Downloaded from www.Manualslib.com manuals search engine

MLD Snooping Global Querier Configuration

Use the MLD Snooping **Global Querier Configuration** page to configure the parameters for the MLD Snooping Querier.

To display the **Global Querier Configuration** page, click **Switching > Multicast Support > MLD Snooping > Global Querier Configuration** in the tree view.

Figure 7-88. MLD Snooping Global Querier Configuration



The MLD Snooping **Global Querier Configuration** page contains the following fields:

- **IP Address—** Specifies the Snooping Querier IPv6 Address which will be used as the source address in periodic MLD queries. This address is used when no address is configured for the VLAN on which the query is being sent.
- **Snooping Querier Admin Mode** — Enables or disables the administrative mode for MLD Snooping for the switch.
- **MLD Version** — Specifies the version of MLD protocol used in periodic MLD queries.
- **Query Interval (1–1800)** — Specifies the time interval in seconds between periodic queries sent by the Snooping Querier. The default value is 60.
- **Expiry Interval (60–300)** — Specifies the time interval in seconds after which the last querier information is removed. The default value is 60.

Configuring Global Querier MLD Snooping Settings with CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the CLI Reference Guide:

- MLD Snooping Commands

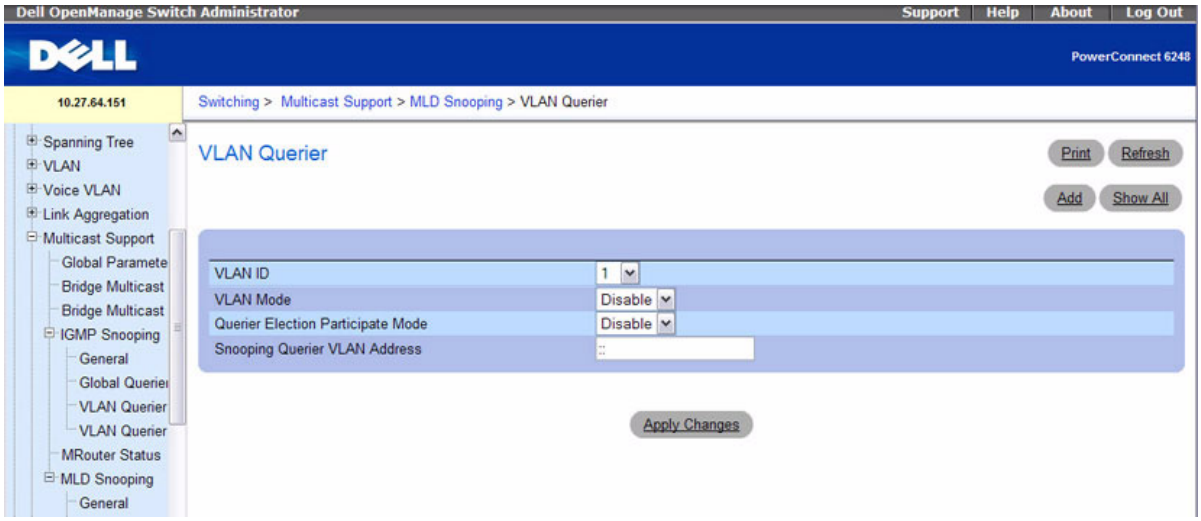
Downloaded from www.Manualslib.com manuals search engine

MLD Snooping VLAN Querier

Use the MLD Snooping **VLAN Querier** page to specify the MLD Snooping Querier settings for individual VLANs.

To display the MLD Snooping **VLAN Querier** page, click **Switching** > **Multicast Support** > **MLD Snooping** > **VLAN Querier** in the tree view.

Figure 7-89. MLD Snooping VLAN Querier



The MLD Snooping **VLAN Querier** page contains the following fields:

- **VLAN ID** — Specifies the VLAN for the MLD Snooping Querier configuration.
- **VLAN Mode** — Enables or disables the MLD Snooping Querier on the VLAN selected in the VLAN ID field.
- **Querier Election Participate Mode** — Enables or disables the MLD participation in election mode by the Snooping Querier. When this mode is disabled, upon seeing another querier of same version in the VLAN, the Snooping Querier transitions to non-querier state. When this mode is enabled, the Snooping Querier participates in querier election, where in the lowest IP address wins the querier election and operates as the querier in that VLAN. The other querier transitions to non-querier state.
- **Snooping Querier VLAN Address** — Specifies the Snooping Querier address to be used as source address in periodic MLD queries sent on the specified VLAN.

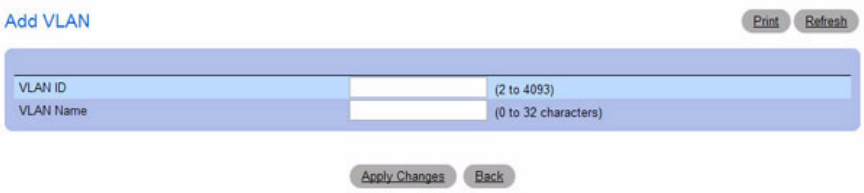
Adding a New VLAN and Configuring the VLAN Querier Settings

1. Open the MLD Snooping **VLAN Querier** page.
2. Click **Add**.

   The page refreshes, and the **Add VLAN** page displays.

Downloaded from www.Manualslib.com manuals search engine

Figure 7-90. Add VLAN Querier



3. Enter the VLAN ID and, if desired, an optional VLAN name.
4. Complete the fields on the page as needed.
5. Click **Apply Changes**.

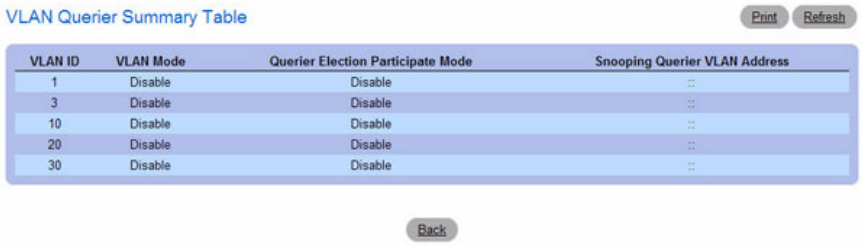
   The VLAN Querier settings are modified, and the device is updated.

Displaying the MLD Snooping VLAN Querier Summary Table

1. Open the MLD Snooping **VLAN Querier** page.
2. Click **Show All**.

   The **VLAN Querier Summary Table** displays.

Figure 7-91. VLAN Querier Summary Table



VLAN ID	VLAN Mode	Querier Election Participate Mode	Snooping Querier VLAN Address
1	Disable	Disable	::
3	Disable	Disable	::
10	Disable	Disable	::
20	Disable	Disable	::
30	Disable	Disable	::

Configuring VLAN Querier Settings with CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the CLI Reference Guide:

- IGMP Snooping Commands

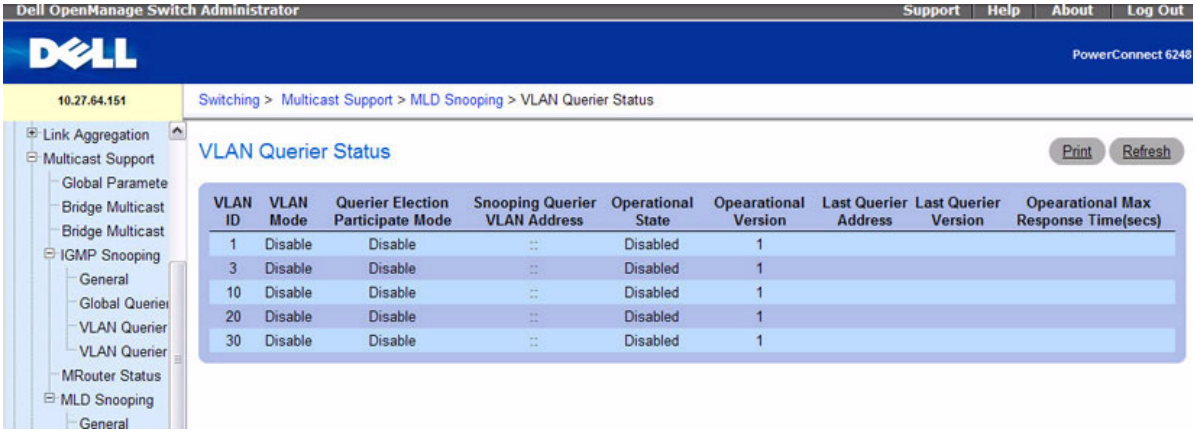
Downloaded from www.Manualslib.com manuals search engine

MLD Snooping VLAN Querier Status

Use the **VLAN Querier Status** page to view the MLD Snooping Querier settings for individual VLANs.

To display the **VLAN Querier Status** page, click **Switching > Multicast Support > MLD Snooping > VLAN Querier Status** in the tree view.

Figure 7-92. MLD Snooping VLAN Querier Status



The MLD Snooping **VLAN Querier Status** page contains the following fields:

- **VLAN ID** — Identifies the VLAN.
- **VLAN Mode** — Shows whether the MLD Snooping Querier is enabled or disabled on the VLAN.
- **Querier Election Participate Mode** — Shows whether the mode is enabled or disabled. When this mode is disabled, upon seeing another querier of same version in the VLAN, the Snooping Querier transitions to non-querier state. When this mode is enabled, the Snooping Querier participates in querier election, where in the lowest IP address wins the querier election and operates as the querier in that VLAN. The other querier transitions to non-querier state.
- **Snooping Querier VLAN Address** — Identifies the Snooping Querier address to be used as source address in periodic MLD queries sent on the VLAN.
- **Operational State** — Displays the operational state of the MLD Snooping Querier on the specified VLAN. It can be in any of the following states:
  - **Querier** — The Snooping switch that is the Querier in the VLAN. The Snooping switch will send out periodic queries with a time interval equal to the configured querier Query Interval. If the Snooping switch sees a better querier in the VLAN, it transitions to non-querier mode.
  - **Non-Querier** — The Snooping switch is in Non-Querier mode in the VLAN. If the querier Expiry Interval timer is expires, the Snooping switch will transition into querier mode.
  - **Disabled** — The Snooping Querier is not operational on the VLAN. The Snooping Querier transitions to disabled mode when 1) MLD Snooping is not operational on the VLAN, 2) the querier address is not configured or 3) the network management address is not configured.
- **Operational Version** — Displays the operational MLD protocol version of the querier.

Downloaded from www.Manualslib.com manuals search engine

- **Last Querier Address** — Displays the IP address of the last querier from which a query was snooped on the VLAN.
- **Last Querier Version** — Displays the MLD protocol version of the last querier from which a query was snooped on the VLAN.
- **Operational Max Response Time** — Displays the maximum response time to be used in the queries that are sent by the Snooping Querier.

Viewing VLAN Querier Status with CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the CLI Reference Guide:

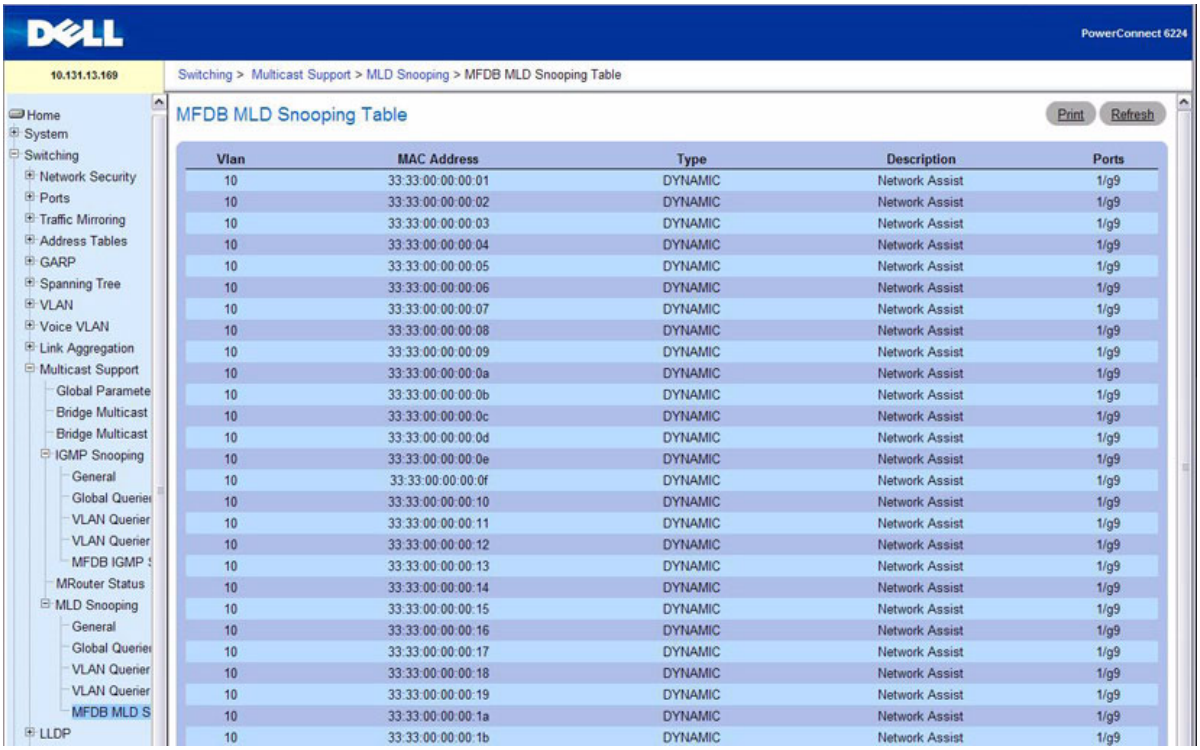
- IGMP Snooping Commands

MFDB MLD Snooping Table

Use the **MFDB MLD Snooping Table** page to view the MFDB MLD Snooping Table settings for individual VLANs.

To display the **MFDB MLD Snooping Table** page, click **Switching > Multicast Support > MLD Snooping > MFDB MLD Snooping Table** in the tree view.

Figure 7-93. MFDB MLD Snooping Table



Vlan	MAC Address	Type	Description	Ports
10	33:33:00:00:00:01	DYNAMIC	Network Assist	1/g9
10	33:33:00:00:00:02	DYNAMIC	Network Assist	1/g9
10	33:33:00:00:00:03	DYNAMIC	Network Assist	1/g9
10	33:33:00:00:00:04	DYNAMIC	Network Assist	1/g9
10	33:33:00:00:00:05	DYNAMIC	Network Assist	1/g9
10	33:33:00:00:00:06	DYNAMIC	Network Assist	1/g9
10	33:33:00:00:00:07	DYNAMIC	Network Assist	1/g9
10	33:33:00:00:00:08	DYNAMIC	Network Assist	1/g9
10	33:33:00:00:00:09	DYNAMIC	Network Assist	1/g9
10	33:33:00:00:00:0a	DYNAMIC	Network Assist	1/g9
10	33:33:00:00:00:0b	DYNAMIC	Network Assist	1/g9
10	33:33:00:00:00:0c	DYNAMIC	Network Assist	1/g9
10	33:33:00:00:00:0d	DYNAMIC	Network Assist	1/g9
10	33:33:00:00:00:0e	DYNAMIC	Network Assist	1/g9
10	33:33:00:00:00:0f	DYNAMIC	Network Assist	1/g9
10	33:33:00:00:00:10	DYNAMIC	Network Assist	1/g9
10	33:33:00:00:00:11	DYNAMIC	Network Assist	1/g9
10	33:33:00:00:00:12	DYNAMIC	Network Assist	1/g9
10	33:33:00:00:00:13	DYNAMIC	Network Assist	1/g9
10	33:33:00:00:00:14	DYNAMIC	Network Assist	1/g9
10	33:33:00:00:00:15	DYNAMIC	Network Assist	1/g9
10	33:33:00:00:00:16	DYNAMIC	Network Assist	1/g9
10	33:33:00:00:00:17	DYNAMIC	Network Assist	1/g9
10	33:33:00:00:00:18	DYNAMIC	Network Assist	1/g9
10	33:33:00:00:00:19	DYNAMIC	Network Assist	1/g9
10	33:33:00:00:00:1a	DYNAMIC	Network Assist	1/g9
10	33:33:00:00:00:1b	DYNAMIC	Network Assist	1/g9

The **MFDB MLD Snooping Table** page contains the following fields:

Downloaded from www.Manualslib.com manuals search engine

- **VLAN** — Displays the VLAN ID associated with an MLD group entry in the MFDB table.
- **MAC Address** — Displays the MAC Address associated with an MLD group entry in the MFDB table.
- **Type** — Displays the type of entry. Static entries are those that are configured by the user. Dynamic entries are added to the table as a result of a learning process or protocol.
- **Description** — The text description of this multicast table entry. Possible values are **Management Configured**, **Network Configured** and **Network Assisted**.
- **Ports** — The list of interfaces that are designated for forwarding (Fwd:) for a corresponding MFDB entry.

Configuring the Link Layer Discovery Protocol (LLDP)

The IEEE 802.1AB defined standard, Link Layer Discovery Protocol (LLDP), allows stations residing on an 802 LAN to advertise major capabilities and physical descriptions. This information is viewed by a network manager to identify system topology and detect bad configurations on the LAN.

LLDP is a one-way protocol; there are no request/response sequences. Information is advertised by stations implementing the transmit function, and is received and processed by stations implementing the receive function. The transmit and receive functions can be enabled/disabled separately per port. By default, both transmit and receive are enabled on all ports. The application is responsible for starting each transmit and receive state machine appropriately, based on the configured status and operational state of the port.

The **LLDP** menu page contains links to the following features:

- LLDP Configuration
- LLDP Statistics
- LLDP Connections

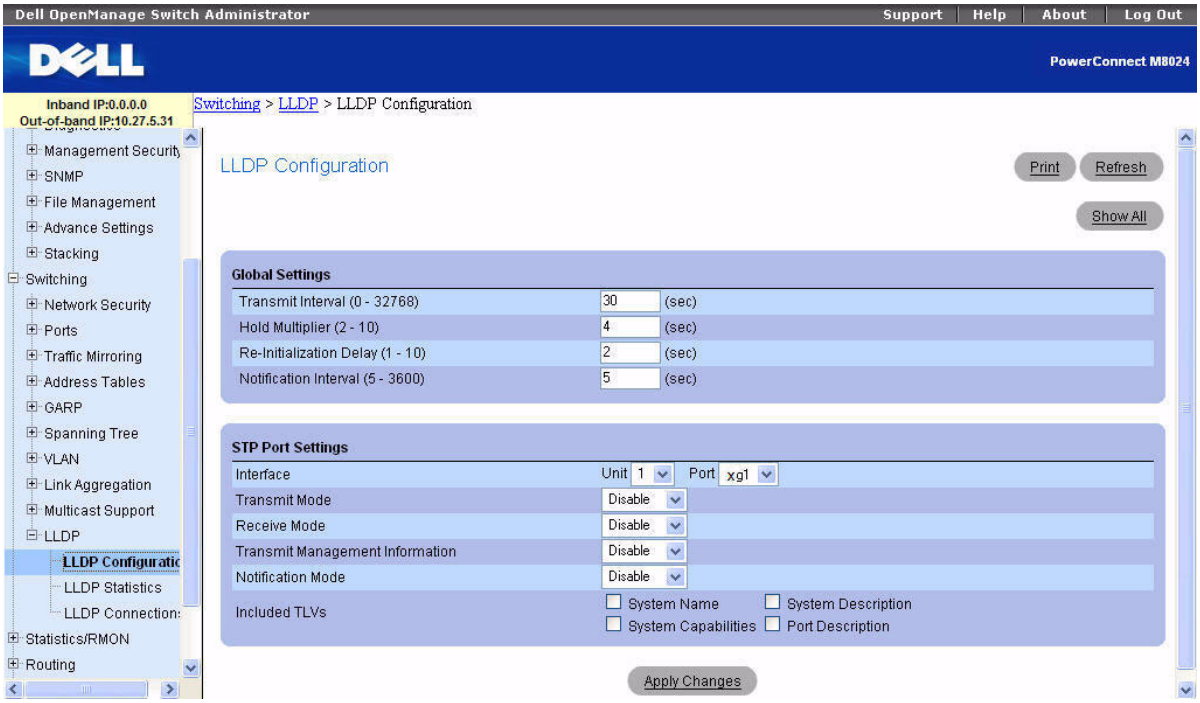
LLDP Configuration

Use the **LLDP Configuration** page to specify LLDP parameters. Parameters that affect the entire system as well as those for a specific interface can be specified here.

To display the **LLDP Configuration** page, click **Switching > LLDP > LLDP Configuration** in the tree view.

Downloaded from www.Manualslib.com manuals search engine

Figure 7-94. LLDP Configuration



The **LLDP Configuration** page contains the following fields:

Global Settings

- **Transmit Interval (1–32768)** — Specifies the interval at which frames are transmitted. The default is 30 seconds.
- **Hold Multiplier (2–10)** — Specifies multiplier on the transmit interval to assign to TTL. Default is 4.
- **Re-Initialization Delay (1–10)** — Specifies delay before a re-initialization. Default is 2 seconds.
- **Notification Interval (5–3600)** — Limits the transmission of notifications. The default is 5 seconds.

Port Settings

- **Interface** — Specifies the port to be affected by these parameters.
- **Transmit Mode** — Enables or disables the transmit function. The default is disabled.
- **Receive Mode** — Enables or disables the receive function. The default is disabled.
- **Transmit Management Information** — Enables or disables transmission of management address instance. Default is disabled.
- **Notification Mode** — Enables or disables remote change notifications. The default is disabled.
- **Included TLVs** — Selects TLV information to transmit. Choices include System Name, System Capabilities, System Description, and Port Description.

Downloaded from www.Manualslib.com manuals search engine

Modifying the LLDP Configuration

1. Open the **LLDP Configuration** page.
2. Define the fields as needed.
3. Click **Apply Changes**.

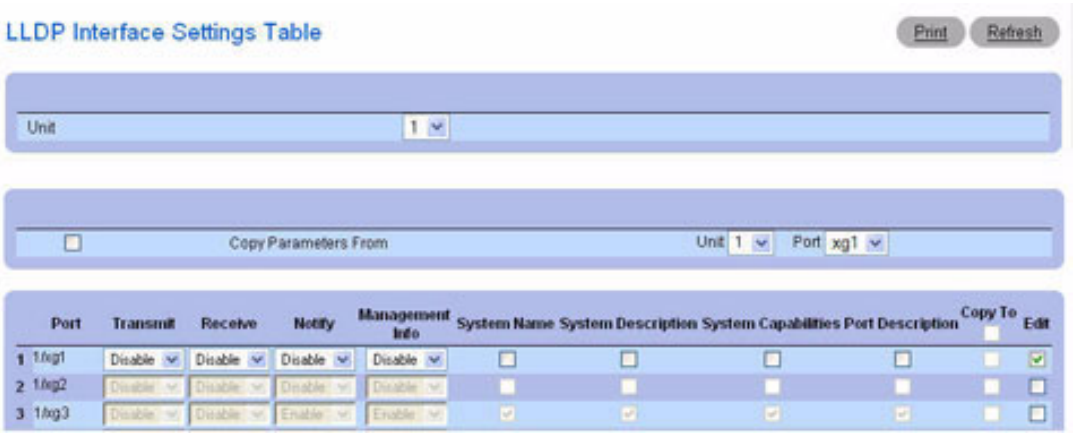
   LLDP parameters are saved to the switch.

Displaying the LLDP Interface Settings Table

1. Open the **LLDP Configuration** page.
2. Click **Show All**.

   The **LLDP Interface Settings Table** displays.

Figure 7-95. LLDP Interface Settings Table



3. Use the **Unit** drop-down menu to view the **LLDP Interface Settings Table** for other units in the stack, if they exist.

Copying LLDP Interface Settings

1. Open the **LLDP Configuration** page.
2. Click **Show All**.

   The **LLDP Interface Settings Table** displays.
3. Specify the Unit and Port you are copying from in **Copy Parameters From**.
4. Click **Copy To** for each Unit/Port to receive these parameters.
5. Click **Apply Changes**.

   The LLDP Interface settings are copied, and the device is updated.

Downloaded from www.Manualslib.com manuals search engine

Modifying LLDP Interface Settings for Multiple Ports

1. Open the **LLDP Configuration** page.
2. Click **Show All**.

   The **LLDP Interface Settings Table** displays.
3. Click **Edit** for each Unit/Port to modify.
4. Edit the LLDP Interface fields as needed.
5. Click **Apply Changes**.

   The LLDP Interface settings are modified, and the device is updated.

Configuring LLDP Configuration with CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

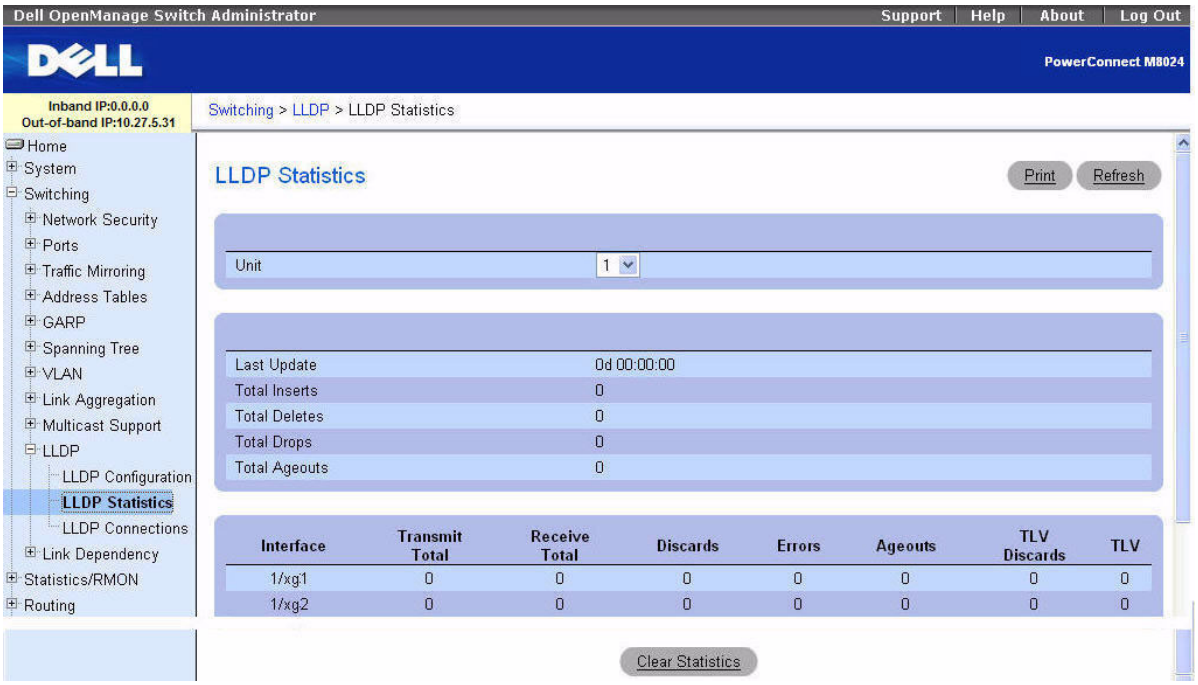
- LLDP Commands

LLDP Statistics

Use the LLDP Statistics page to view LLPD-related statistics.

To display the **LLDP Statistics** page, click **Switching > LLDP > LLDP Statistics** in the tree view.

Figure 7-96. LLDP Statistics



Downloaded from www.Manualslib.com manuals search engine

The **LLDP Statistics** page displays the following statistics:

System-wide Statistics

- **Last Update** — Displays the value of system up time the last time a remote data entry was created, modified, or deleted.
- **Total Inserts** — Displays the number of times a complete set of information advertised by a remote switch has been inserted into the table.
- **Total Deletes** — Displays the number of times a complete set of information advertised by a remote switch has been deleted from the table.
- **Total Drops** — Displays the number of times a complete set of information advertised by a remote switch could not be inserted due to insufficient resources.
- **Total Ageouts** — Displays the number of times any remote data entry has been deleted due to TTL (Time-to-Live) expiration.

Port Statistics

- **Interface** — Displays the Unit and Port to which the statistics on that line apply.
- **Transmit Total** — Displays the total number of LLDP frames transmitted on the indicated port.
- **Receive Total** — Displays the total number of valid LLDP frames received on the indicated port.
- **Discards** — Displays the number of LLDP frames received on the indicated port and discarded for any reason.
- **Errors —** Displays the number of invalid LLDP frames received on the indicated port.
- **Ageouts** — Displays the number of times a remote data entry on the indicated port has been deleted due to TTL expiration.
- **TLV Discards** — Displays the number of LLDP TLVs (Type, Length, Value sets) received on the indicated port and discarded for any reason by the LLDP agent.
- **TLV Unknowns** — Displays the number of LLDP TLVs received on the indicated port for a type not recognized by the LLDP agent.

Use the **Unit** drop-down menu to view the **LLDP Statistics** for other units in the stack, if they exist.

Use the **Clear Statistics** button to reset all LLDP Statistics to zero.

Displaying LLDP Statistics with the CLI Command

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- LLDP Commands

Downloaded from www.Manualslib.com manuals search engine

LLDP Connections

Use the **LLDP Connections** page to view the list of ports with LLDP enabled. Basic connection details are displayed.

To display the **LLDP Connections** page, click **Switching > LLDP > LLDP Connections** in the tree view.

Figure 7-97. LLDP Connections Table

The **LLDP Connections** page displays the following port details:

- **Local Interface** — Designates a unit and port in the stack.
- **Chassis ID** — Identifies the 802 LAN device's chassis.
- **Port ID** — Identifies the port number from which the LLDPDU is transmitted.
- **System Name** — Identifies the system name associated with the remote device.

Use the **Unit** drop-down menu to view the **LLDP Connections** for other units in the stack, if they exist.

Use the **Clear Table** button to delete all information from the **LLDP Connections** table.

Downloaded from www.Manualslib.com manuals search engine

Viewing Details about the LLDP Connections

1. Open the **LLDP Connections** page.
2. Click the interface in the **Local Interface** field to view details about that device.

   The **LLDP Connections - Detailed** page for the device displays.

Figure 7-98. Detailed LLDP Connections

3. Use the **Back** button to return to the **LLDP Connections** page.

Viewing LLDP Connections with the CLI Command

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- LLDP Commands

Downloaded from www.Manualslib.com manuals search engine

Creating Link Dependencies

The link dependency feature provides the ability to enable or disable one or more ports based on the link state of one or more different ports. With link dependency enabled on a port, the link state of that port is dependent on the link state of another port. For example, if port A is dependent on port B and the switch detects a link loss on port B, the switch automatically brings down the link on port A. When the link is restored to port B, the switch automatically restores the link to port A.

You can create a maximum of 72 dependency groups. The ports participating in the Link Dependency can be across all the Stack Units (Manager/Member unit).

The Link Dependency feature supports the following scenarios:

- Port dependent on port — If a port loses the link, the switch brings down the link on another port.
- Port dependent on LAG — If all ports in a channel-group lose the link, the switch brings down the link on another port.
- LAG dependent on port — If a port loses the link, the switch brings down all links in a channel-group.
- Multiple port command — If a group of ports lose their link, the switch brings down the link on another group of ports.
- Overlapping ports — Overlapping ports on different groups will be brought down only if both dependent ports lose the link.

The **Link Dependency** menu page contains a link to the Link Dependency Summary page.

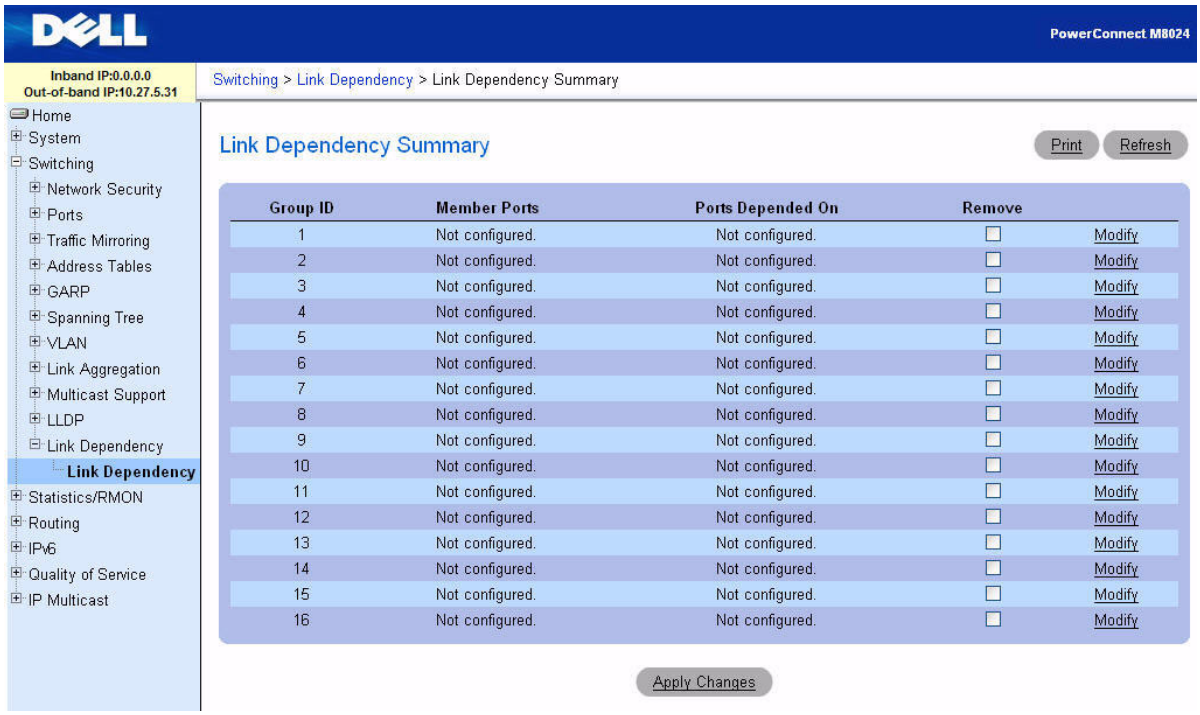
Link Dependency Summary

Use the **Link Dependency Summary** page to view all link dependencies on the system and to access the **Link Dependency Configuration** page. You can create a maximum of 16 dependency groups. The page displays the groups whether they have been configured or not.

To display the **Link Dependency Summary** page, click **Switching > Link Dependency > Link Dependency Summary** in the tree view.

Downloaded from www.Manualslib.com manuals search engine

Figure 7-99. Link Dependency Summary



Group ID	Member Ports	Ports Depended On	Remove	
1	Not configured.	Not configured.	☐	Modify
2	Not configured.	Not configured.	☐	Modify
3	Not configured.	Not configured.	☐	Modify
4	Not configured.	Not configured.	☐	Modify
5	Not configured.	Not configured.	☐	Modify
6	Not configured.	Not configured.	☐	Modify
7	Not configured.	Not configured.	☐	Modify
8	Not configured.	Not configured.	☐	Modify
9	Not configured.	Not configured.	☐	Modify
10	Not configured.	Not configured.	☐	Modify
11	Not configured.	Not configured.	☐	Modify
12	Not configured.	Not configured.	☐	Modify
13	Not configured.	Not configured.	☐	Modify
14	Not configured.	Not configured.	☐	Modify
15	Not configured.	Not configured.	☐	Modify
16	Not configured.	Not configured.	☐	Modify

The **Link Dependency Summary** page contains the following fields:

- **Group ID** — The ID number of the group.
- **Member Ports** — The list of member ports belonging to the group.
- **Ports Depended On** — The list of ports upon which the group depends.
- **Remove** — A check box for removing the configuration for a group.
- **Modify** — A link for modifying the configuration of a group. Click the Modify link to access the configuration page for the group.

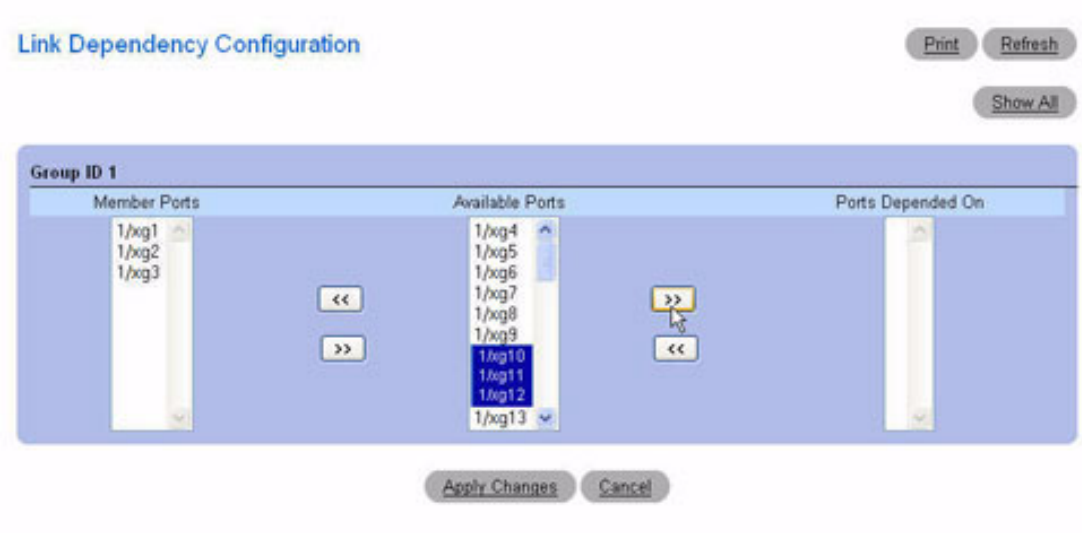
Modifying a Link Dependency Group

1. Open the **Link Dependency Summary** page.
2. From the Group ID row for the Link Dependency group to configure, click the **Modify** link.

   The **Link Dependency Group Configuration** page displays.

Downloaded from www.Manualslib.com manuals search engine

Figure 7-100. Link Dependency Group Configuration



3. To add a port to the **Member Ports** column, click the port in the **Available Ports** column, and then click the << button to the left of the **Available Ports** column. Ctrl + click to select multiple ports.
4. To add a port to the **Ports Depended On** column, click the port in the **Available Ports** column, and then click the >> button to the right of the **Available Port**s column.
5. Click **Apply Changes**.

   The Link Dependency settings for the group are modified, and the device is updated.
6. Click **Show All** to return to the **Link Dependency Summary** page.

Removing All Ports From a Link Dependency Group

1. Open the **Link Dependency Summary** page.
2. From the Group ID row for the Link Dependency group to remove, select the **Remove** check box.
3. Click **Apply Changes**.

   The all ports are removed from the Link Dependency group, and the device is updated.

Configuring Link Dependency Groups With CLI Commands

For information about the CLI commands that perform this function, refer to the following chapter in the *CLI Reference Guide*:

- Link Dependency Commands

Downloaded from www.Manualslib.com manuals search engine

Dynamic ARP Inspection

Dynamic ARP Inspection (DAI) is a security feature that rejects invalid and malicious ARP packets. DAI prevents a class of man-in-the-middle attacks, where an unfriendly station intercepts traffic for other stations by poisoning the ARP caches of its unsuspecting neighbors. The miscreant sends ARP requests or responses mapping another station's IP address to its own MAC address.

DAI relies on DHCP snooping. DHCP snooping listens to DHCP message exchanges and builds a binding database of valid {MAC address, IP address, VLAN, and interface} tuples.

When DAI is enabled, the switch drops ARP packets whose sender MAC address and sender IP address do not match an entry in the DHCP snooping bindings database. You can optionally configure additional ARP packet validation.

The **Dynamic ARP Inspection** menu page contains links to the following features:

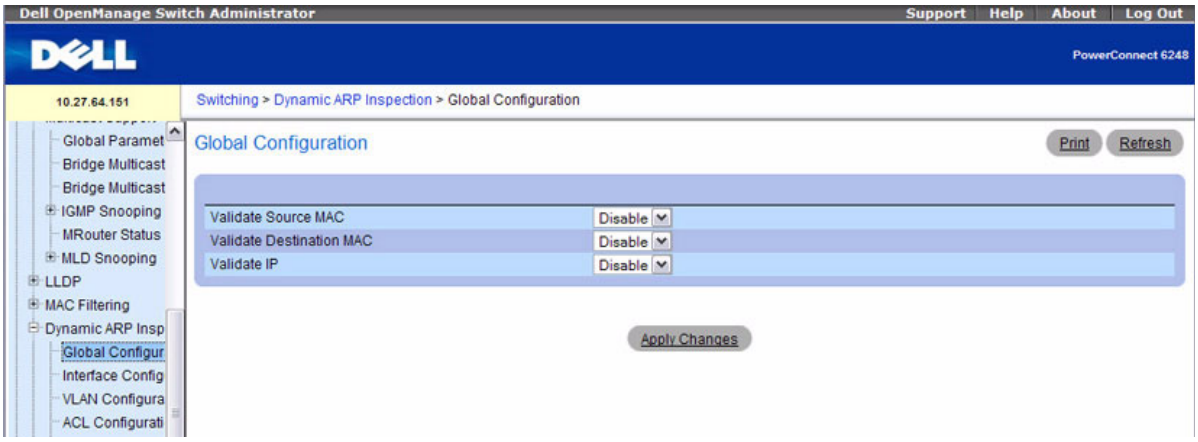
- DAI Global Configuration
- DAI Interface Configuration
- DAI VLAN Configuration
- DAI ACL Configuration
- DAI ACL Rule Configuration
- DAI Statistics

DAI Global Configuration

Use the DAI Configuration page to configure global DAI settings.

To display the DAI Configuration page, click **Switching > Dynamic ARP Inspection > Global Configuration** in the navigation tree.

Figure 7-101. Dynamic ARP Inspection Global Configuration



Downloaded from www.Manualslib.com manuals search engine

The **Dynamic ARP Inspection Global Configuration** page contains the following fields:

- **Validate Source MAC** — Select the DAI Source MAC Validation Mode for the switch. If you select Enable, Sender MAC validation for the ARP packets will be enabled. The default is Disable.
- **Validate Destination MAC**—Select the DAI Destination MAC Validation Mode for the switch. If you select Enable, Destination MAC validation for the ARP Response packets will be enabled. The default is Disable.
- **Validate IP**—Select the DAI IP Validation Mode for the switch. If you select Enable, IP Address validation for the ARP packets will be enabled. The default is Disable.

Configuring Dynamic ARP Inspection With CLI Commands

For information about the CLI commands that perform this function, refer to the following chapter in the *CLI Reference Guide*:

- Dynamic ARP Inspection Commands

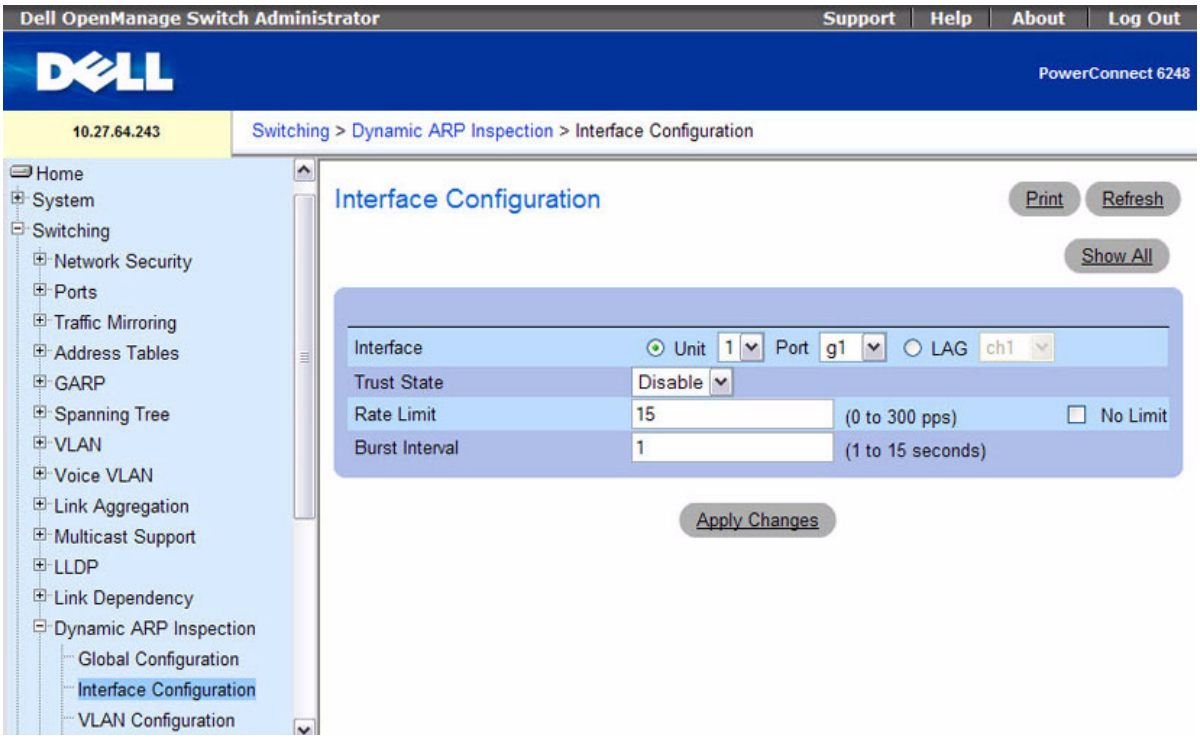
DAI Interface Configuration

Use the DAI Interface Configuration page to select the DAI Interface for which information is to be displayed or configured.

To display the DAI Interface Configuration page, click **Switching > Dynamic ARP Inspection > DAI Interface Configuration** in the navigation tree.

Downloaded from www.Manualslib.com manuals search engine

Figure 7-102. Dynamic ARP Inspection Interface Configuration



The **Dynamic ARP Inspection Interface Configuration** page contains the following fields:

- **Port**— Select the port or LAG for which data is to be displayed or configured.
- **Trust State** — Indicates whether the interface is trusted for Dynamic ARP Inspection. If you select Enable, the interface is trusted. ARP packets coming to this interface will be forwarded without checking. If you select Disable, the interface is not trusted. ARP packets coming to this interface will be subjected to ARP inspection. The default is Disable.
- **Rate Limit** — Specify the rate limit value for Dynamic ARP Inspection. If the incoming rate exceeds the Rate Limit value for consecutively burst interval seconds, ARP packets will be dropped. Use the corresponding check box to set No Limit. The default is 15 packets per second (pps).
- **Burst Interval** — Specify the burst interval for rate limiting on this interface. If the Rate Limit is None, then Burst Interval has no meaning and shows as N/A (Not Applicable). The default is 1 second.

Configuring Dynamic ARP Inspection With CLI Commands

For information about the CLI commands that perform this function, refer to the following chapter in the *CLI Reference Guide*:

- Dynamic ARP Inspection Commands

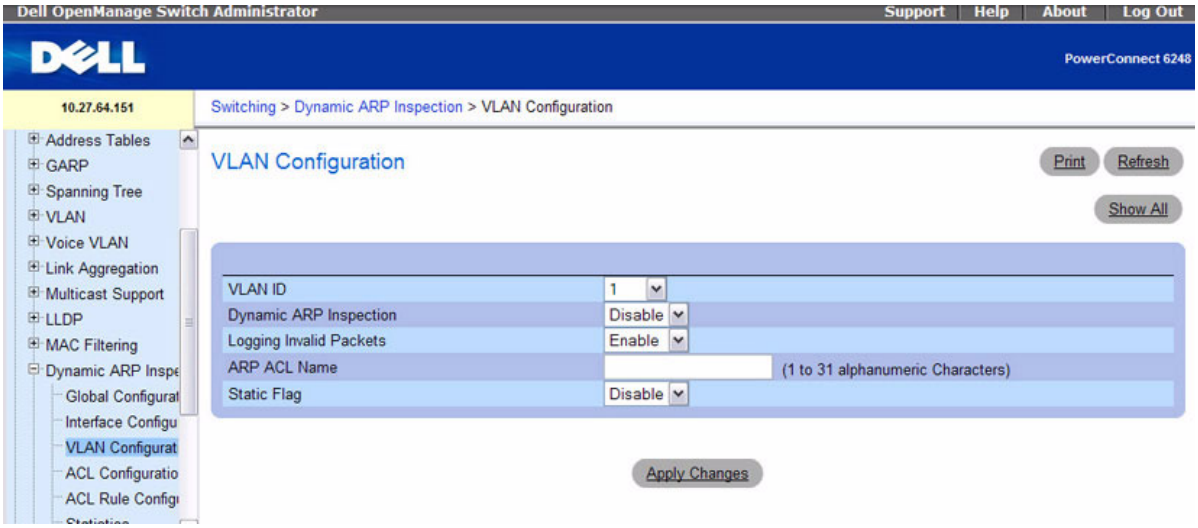
Downloaded from www.Manualslib.com manuals search engine

DAI VLAN Configuration

Use the DAI VLAN Configuration page to select the DAI-capable VLANs for which information is to be displayed or configured.

To display the DAI VLAN Configuration page, click **Switching > Dynamic ARP Inspection > VLAN Configuration** in the navigation tree.

Figure 7-103. Dynamic ARP Inspection VLAN Configuration



The **Dynamic ARP Inspection VLAN Configuration** page contains the following fields:

- **VLAN ID** — Select the VLAN ID for which information is to be displayed or configured.
- **Dynamic ARP Inspection** — Select whether Dynamic ARP Inspection is Enabled or Disabled on this VLAN. The default is Disable.
- **Logging Invalid Packets** — Select whether Dynamic ARP Inspection logging is Enabled or Disabled on this VLAN. The default is Disable.
- **ARP ACL Name** — The name of the ARP Access List. A VLAN can be configured to use this ARP ACL containing rules as the filter for ARP packet validation. The name can contain 1-31 alphanumeric characters.
- **Static Flag** — Use this flag to determine whether the ARP packet needs validation using the DHCP snooping database, in case the ARP ACL rules do not match. If Enabled, then the ARP Packet will be validated by the ARP ACL Rules only. If Disabled, then the ARP Packet needs further validation by using the DHCP Snooping entries. The default is Disable.

Downloaded from www.Manualslib.com manuals search engine

Configuring Dynamic ARP Inspection With CLI Commands

For information about the CLI commands that perform this function, refer to the following chapter in the *CLI Reference Guide*:

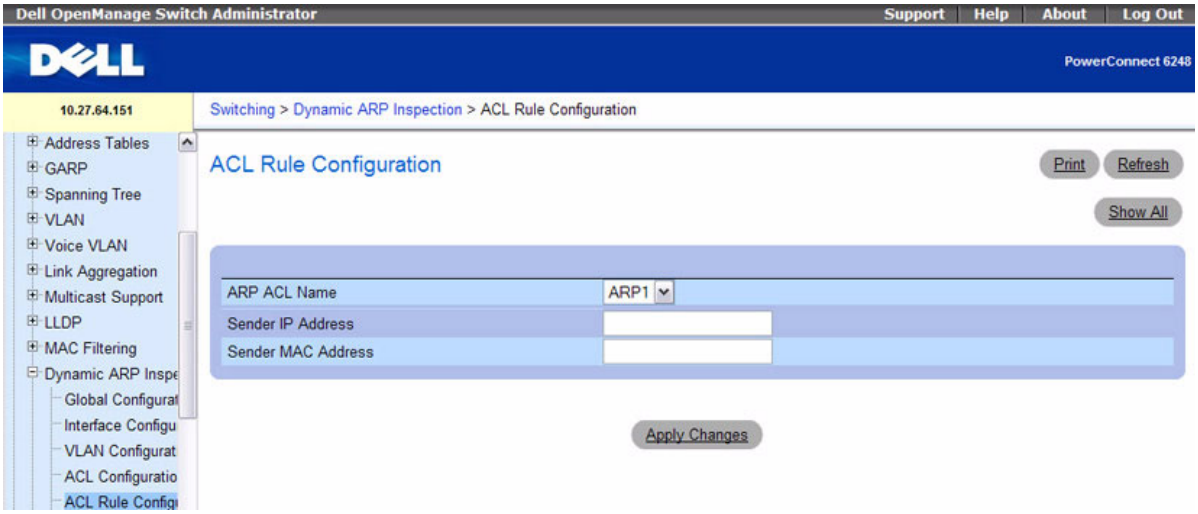
- Dynamic ARP Inspection Commands

DAI ACL Configuration

Use the DAI ARP ACL Configuration page to add or remove DAI ARP ACLs.

To display the DAI ARP ACL Configuration page, click **Switching > Dynamic ARP Inspection > ACL Configuration** in the navigation tree.

Figure 7-104. Dynamic ARP Inspection ARP ACL Configuration



The **Dynamic ARP Inspection ARP ACL Configuration** page contains the following field:

- **ARP ACL Name** — Use this field to create a new ARP ACL for Dynamic ARP Inspection. The name can be 1 to 31 alphanumeric characters in length.

Configuring Dynamic ARP Inspection With CLI Commands

For information about the CLI commands that perform this function, refer to the following chapter in the *CLI Reference Guide*:

- Dynamic ARP Inspection Commands

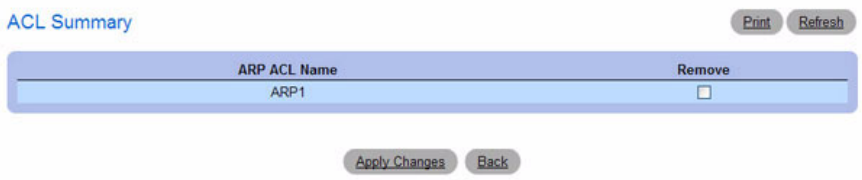
Downloaded from www.Manualslib.com manuals search engine

Displaying the DAI ACL Summary Table and Removing an Entry

1. Open the **DAI ACL Configuration** page.
2. Click **Show All**.

   The **Dynamic ARP Inspection ACL Summary** table displays.

Figure 7-105. Dynamic ARP Inspection ACL Summary



3. To remove an ARP ACL from the list, select the Remove option in the appropriate row, and then click **Apply Changes**.

Configuring Dynamic ARP Inspection With CLI Commands

For information about the CLI commands that perform this function, refer to the following chapter in the *CLI Reference Guide*:

- Dynamic ARP Inspection Commands

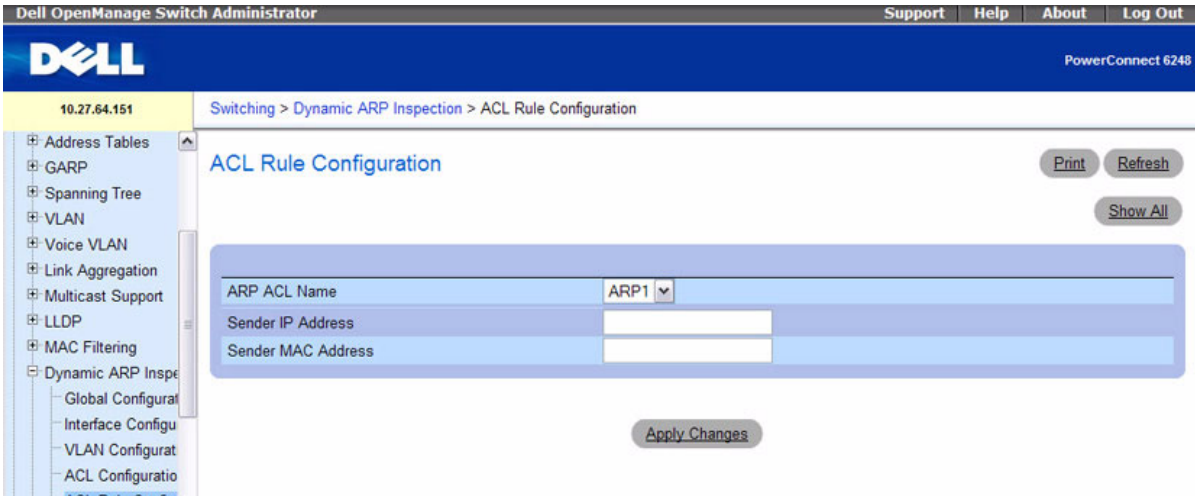
DAI ACL Rule Configuration

Use the DAI ARP ACL Rule Configuration page to add or remove DAI ARP ACL Rules.

To display the DAI ARP ACL Rule Configuration page, click **Switching > Dynamic ARP Inspection > ACL Rule Configuration** in the navigation tree.

Downloaded from www.Manualslib.com manuals search engine

Figure 7-106. Dynamic ARP Inspection Rule Configuration



The **Dynamic ARP Inspection Rule Configuration** page contains the following fields:

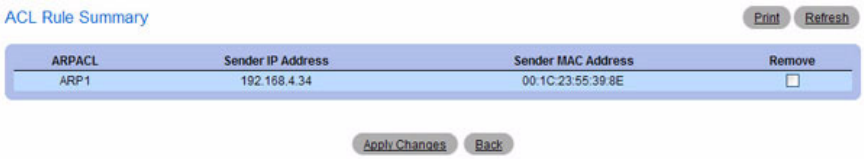
- **ARP ACL Name** — Select the ARP ACL for which information is to be displayed or configured.
- **Sender IP Address** — To create a new rule for the selected ARP ACL, enter in this field the Sender IP Address match value for the ARP ACL.
- **Sender MAC Address** — To create a new rule for the selected ARP ACL, enter in this field the Sender MAC Address match value for the ARP ACL.

Displaying the DAI ACL Rule Summary Table

1. Open the **DAI ACL Rule Configuration** page.
2. Click **Show All**.

   The **Dynamic ARP Inspection ACL Rule Summary** table displays.

Figure 7-107. Dynamic ARP Inspection Rule Summary



Configuring Dynamic ARP Inspection With CLI Commands

For information about the CLI commands that perform this function, refer to the following chapter in the *CLI Reference Guide*:

- Dynamic ARP Inspection Commands

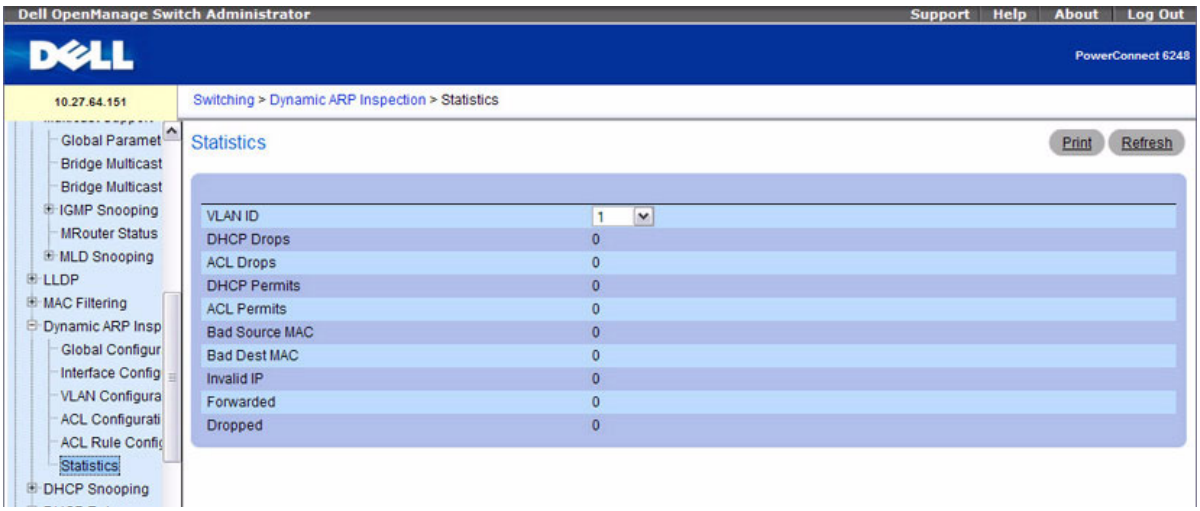
Downloaded from www.Manualslib.com manuals search engine

DAI Statistics

Use the DAI Statistics page to display the statistics per VLAN.

To display the DAI Statistics page, click **Switching > Dynamic ARP Inspection > Statistics** in the navigation tree.

Figure 7-108. Dynamic ARP Inspection Statistics



The **Dynamic ARP Inspection Statistics** page contains the following fields:

- **VLAN ID** — Select the DAI-enabled VLAN ID for which to display statistics.
- **DHCP Drops** — The number of ARP packets that were dropped by DAI because there was no matching DHCP snooping binding entry found.
- **ACL Drops** — The number of ARP packets that were dropped by DAI because there was no matching ARP ACL rule found for this VLAN and the static flag is set on this VLAN.
- **DHCP Permits** — The number of ARP packets that were forwarded by DAI because there was a matching DHCP snooping binding entry found.
- **ACL Permits** — The number of ARP packets that were permitted by DAI because there was a matching ARP ACL rule found for this VLAN.
- **Bad Source MAC** — The number of ARP packets that were dropped by DAI because the sender MAC address in the ARP packet did not match the source MAC in the Ethernet header.
- **Bad Dest MAC** — The number of ARP packets that were dropped by DAI because the target MAC address in the ARP reply packet did not match the destination MAC in the Ethernet header.
- **Invalid IP** — The number of ARP packets dropped by DAI because the sender IP address in the ARP packet or target IP address in the ARP reply packet is not valid. Invalid addresses include 0.0.0.0, 255.255.255.255, IP multicast addresses, class E addresses (240.0.0.0/4), and loopback addresses (127.0.0.0/8).
- **Forwarded** — The number of valid ARP packets forwarded by DAI.

Downloaded from www.Manualslib.com manuals search engine

- **Dropped** — The number of not valid ARP packets dropped by DAI.

Configuring Dynamic ARP Inspection With CLI Commands

For information about the CLI commands that perform this function, refer to the following chapter in the *CLI Reference Guide*:

- Dynamic ARP Inspection Commands

DHCP Snooping

DHCP snooping is a security feature that monitors DHCP messages between a DHCP client and DHCP servers to filter harmful DHCP messages and to build a bindings database of MAC address, IP address, VLAN ID, and port tuples that are considered authorized. You can enable DHCP snooping globally, per-interface, and on specific VLANs, and configure ports within the VLAN to be trusted or untrusted. DHCP servers must be reached through trusted ports.

DHCP snooping enforces the following security rules:

- DHCP packets from a DHCP server (DHCPOFFER, DHCPACK, DHCPNAK, DHCPRELEASEQUERY) are dropped if received on an untrusted port.
- DHCPRELEASE and DHCPDECLINE messages are dropped if for a MAC address in the snooping database, but the binding's interface is other than the interface where the message was received.
- On untrusted interfaces, the switch drops DHCP packets whose source MAC address does not match the client hardware address. This feature is a configurable option.

The hardware identifies all incoming DHCP packets on ports where DHCP snooping is enabled. DHCP snooping is enabled on a port if (a) DHCP snooping is enabled globally, and (b) the port is a member of a VLAN where DHCP snooping is enabled. On untrusted ports, the hardware traps all incoming DHCP packets to the CPU. On trusted ports, the hardware forwards client messages and copies server messages to the CPU so that DHCP snooping can learn the binding.

Table 7-3. DHCP Snooping

	Destination UDP Port 67 (from client)	Destination UDP Port 68 (from server)
Trusted Port	Forward in hardware	Copy to CPU (Complete the tentative binding for a given DHCP client, based on the MAC address.)
Untrusted Port	Trap to CPU (enforcement)	Trap to CPU (error logging)

To display the **DHCP Snooping** page, click **Switching > DHCP Snooping** in the tree view.

The **DHCP Snooping** menu page contains links to the following features:

- DHCP Snooping Configuration
- DHCP Snooping Interface Configuration
- DHCP Snooping VLAN Configuration

Downloaded from www.Manualslib.com manuals search engine

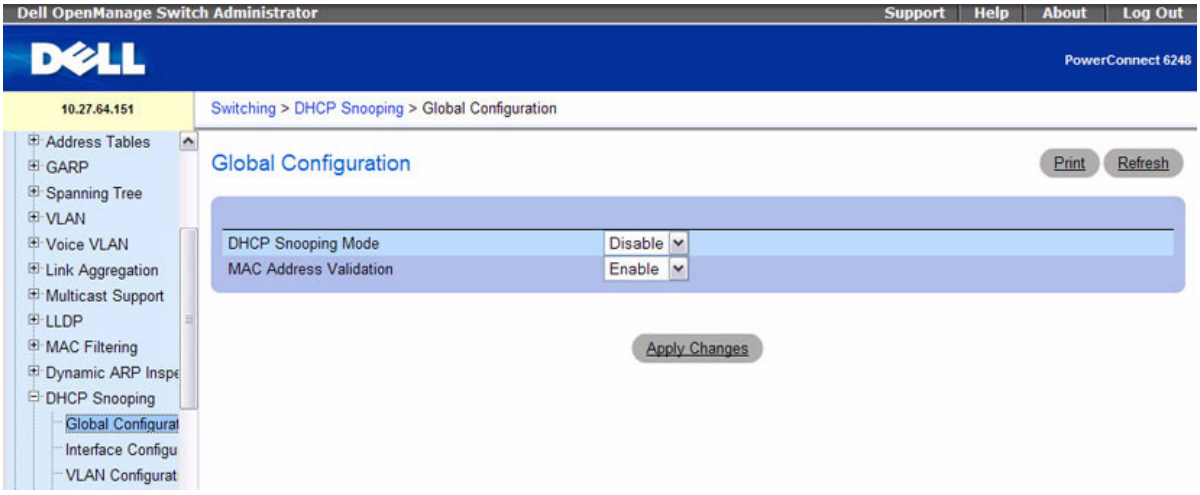
- DHCP Snooping Persistent Configuration
- DHCP Snooping Static Bindings Configuration
- DHCP Snooping Dynamic Bindings Summary
- DHCP Snooping Statistics
- IP Source Guard

DHCP Snooping Configuration

Use the DHCP Snooping Configuration page to control the DHCP Snooping mode on the switch and to specify whether the sender MAC Address for DHCP Snooping must be validated.

To access the DHCP Snooping Configuration page, click **Switching > DHCP Snooping > Global Configuration** in the navigation tree.

Figure 7-109. DHCP Snooping Configuration



The **DHCP Snooping Configuration** page contains the following fields:

- **DHCP Snooping Mode** — Enables or disables the DHCP Snooping feature. The default is Disable.
- **MAC Address Validation** — Enables or disables the validation of sender MAC Address for DHCP Snooping. The default is Enable.

Configuring DHCP Snooping With CLI Commands

For information about the CLI commands that perform this function, refer to the following chapter in the *CLI Reference Guide*:

- DHCP Snooping Commands

Downloaded from www.Manualslib.com manuals search engine

DHCP Snooping Interface Configuration

Use the **DHCP Snooping Interface Configuration** page to configure the DHCP Snooping settings on individual interfaces.

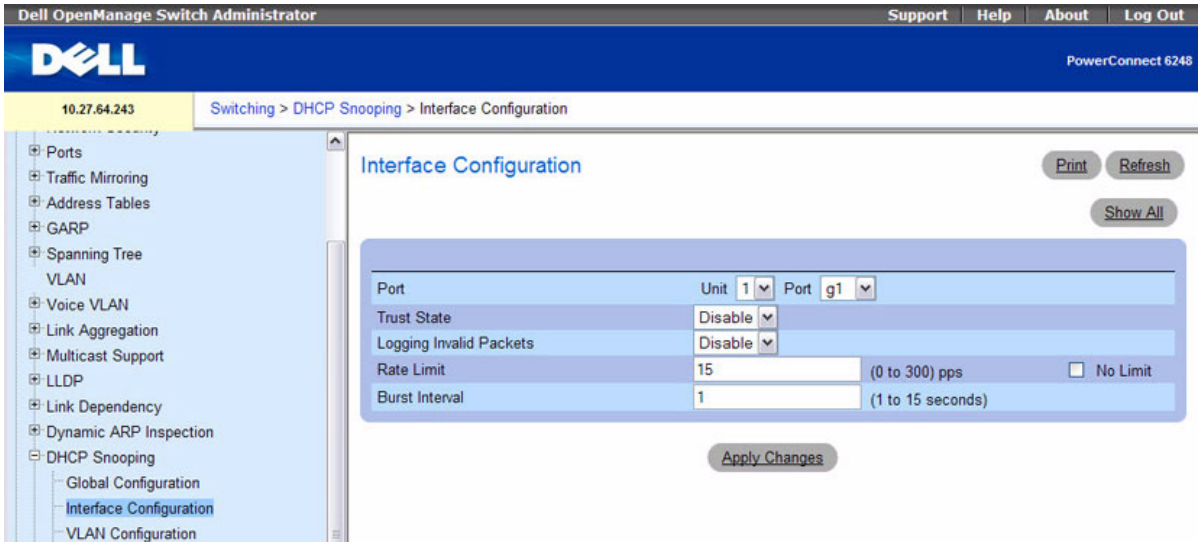
The hardware rate limits DHCP packets sent to the CPU from untrusted interfaces to 64 Kbps. There is no hardware rate limiting on trusted interfaces.

To prevent DHCP packets from being used as a DoS attack when DHCP snooping is enabled, the snooping application enforces a rate limit for DHCP packets received on untrusted interfaces. DHCP snooping monitors the receive rate on each interface separately. If the receive rate exceeds the configuration limit, DHCP snooping brings down the interface. The port must be administratively enabled from the **Switching > Ports > Port Configuration** page (or the `no shutdown` CLI command) to further work with the port. You can configure both the rate and the burst interval.

The DHCP snooping application processes incoming DHCP messages. For DHCPRELEASE and DHCPDECLINE messages, the application compares the receive interface and VLAN with the client's interface and VLAN in the binding database. If the interfaces do not match, the application logs the event and drops the message. For valid client messages, DHCP snooping compares the source MAC address to the DHCP client hardware address. Where there is a mismatch, DHCP snooping logs and drops the packet. You can disable this feature using the **DHCP Snooping Interface Configuration** page or by using the `no ip dhcp snooping verify mac-address` command. DHCP snooping forwards valid client messages on trusted members within the VLAN. If DHCP relay and/or DHCP server co-exist with the DHCP snooping, the DHCP client message will be sent to the DHCP relay and/or DHCP server to process further.

To access the **DHCP Snooping Interface Configuration** page, click **Switching > DHCP Snooping > Interface Configuration** in the navigation tree.

Figure 7-110. DHCP Snooping Interface Configuration



Downloaded from www.Manualslib.com manuals search engine

The **DHCP Snooping Interface Configuration** page contains the following fields:

- **Port** — Select the interface for which data is to be displayed or configured.
- **Trust State** — If it is enabled, the DHCP snooping application considers the port as trusted. The default is Disable.
- **Logging Invalid Packets** — If it is enabled, the DHCP snooping application logs invalid packets on this interface. The default is Disable.
- **Rate Limit** — Specifies the rate limit value for DHCP snooping purposes. If the incoming rate of DHCP packets exceeds the value of this object for consecutively burst interval seconds, the port will be shutdown. If this value is None, there is no limit. The default is 15 packets per second (pps). The Rate Limit range is 0 to 300.
- **No Limit** — Specifies the value of Rate Limit which is -1. If the rate limit is -1, burst interval has no meaning and is therefore disabled.
- **Burst Interval** — Specifies the burst interval value for rate limiting purposes on this interface. If the rate limit is None, the burst interval has no meaning and displays it as "N/A". The default is 1 second. The Burst Interval range is 1 to 15.

Displaying the DHCP Snooping Interface Summary Table

1. Open the **DHCP Snooping Interface Configuration** page.
2. Click **Show All**.

   The **DHCP Snooping Interface Summary** table displays.

Figure 7-111. DHCP Snooping Interface Summary

DHCP Snooping Interface Summary

Print Refresh

Interface	Trust State	Logging Invalid Packets	Rate Limit	Burst Interval
1/g1	Disable	Disable	15	1
1/g2	Disable	Disable	15	1
1/g3	Disable	Disable	15	1
1/g4	Disable	Disable	15	1
1/g5	Disable	Disable	15	1
1/g6	Disable	Disable	15	1
1/g7	Disable	Disable	15	1
1/g8	Disable	Disable	15	1
1/g9	Disable	Disable	15	1
1/g10	Disable	Disable	15	1
1/g11	Disable	Disable	15	1
1/g12	Disable	Disable	15	1

Configuring DHCP Snooping With CLI Commands

For information about the CLI commands that perform this function, refer to the following chapter in the *CLI Reference Guide*:

- DHCP Snooping Commands

Downloaded from www.Manualslib.com manuals search engine

DHCP Snooping VLAN Configuration

The DHCP snooping application does not forward server messages because they are forwarded in hardware.

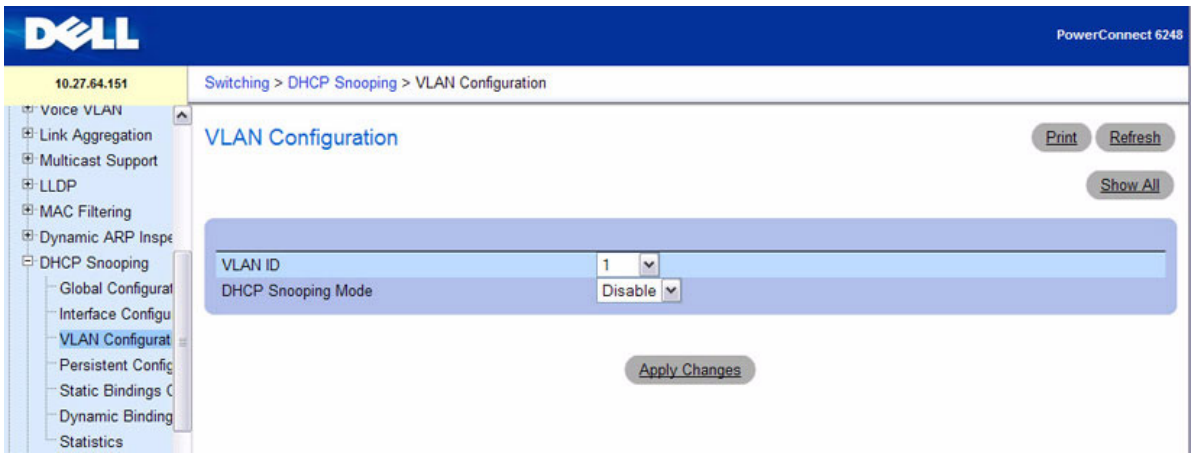
DHCP snooping forwards valid DHCP client messages received on non-routing VLANs. The message is forwarded on all trusted interfaces in the VLAN.

DHCP snooping can be configured on switching VLANs and routing VLANs. When a DHCP packet is received on a routing VLAN, the DHCP snooping application applies its filtering rules and updates the bindings database. If a client message passes filtering rules, the message is placed into the software forwarding path, where it may be processed by the DHCP relay agent, the local DHCP server, or forwarded as an IP packet.

DHCP snooping is disabled globally and on all VLANs by default. Ports are untrusted by default.

To access the DHCP Snooping VLAN Configuration page, click **Switching > DHCP Snooping > VLAN Configuration** in the navigation tree.

Figure 7-112. DHCP Snooping VLAN Configuration



The **DHCP Snooping VLAN Configuration** page contains the following fields:

- **VLAN ID** — Select the VLAN for which information to be displayed or configured for the DHCP snooping application.
- **DHCP Snooping Mode** — Enables or disables the DHCP snooping feature on the selected VLAN. The default is Disable.

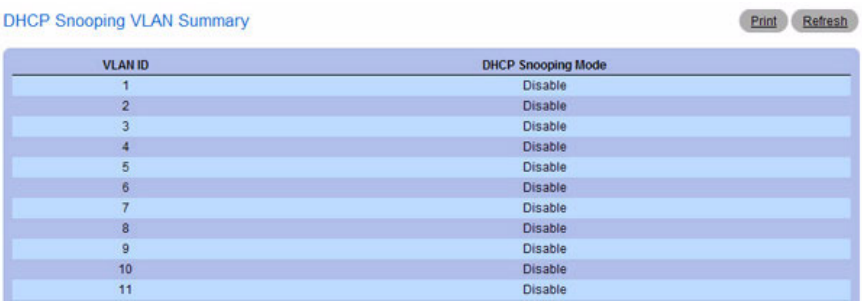
Displaying the DHCP Snooping VLAN Summary Table

1. Open the **DHCP Snooping VLAN Configuration** page.
2. Click **Show All**.

   The **DHCP Snooping VLAN Summary** table displays.

Downloaded from www.Manualslib.com manuals search engine

Figure 7-113. DHCP Snooping VLAN Summary



VLAN ID	DHCP Snooping Mode
1	Disable
2	Disable
3	Disable
4	Disable
5	Disable
6	Disable
7	Disable
8	Disable
9	Disable
10	Disable
11	Disable

Configuring DHCP Snooping With CLI Commands

For information about the CLI commands that perform this function, refer to the following chapter in the *CLI Reference Guide*:

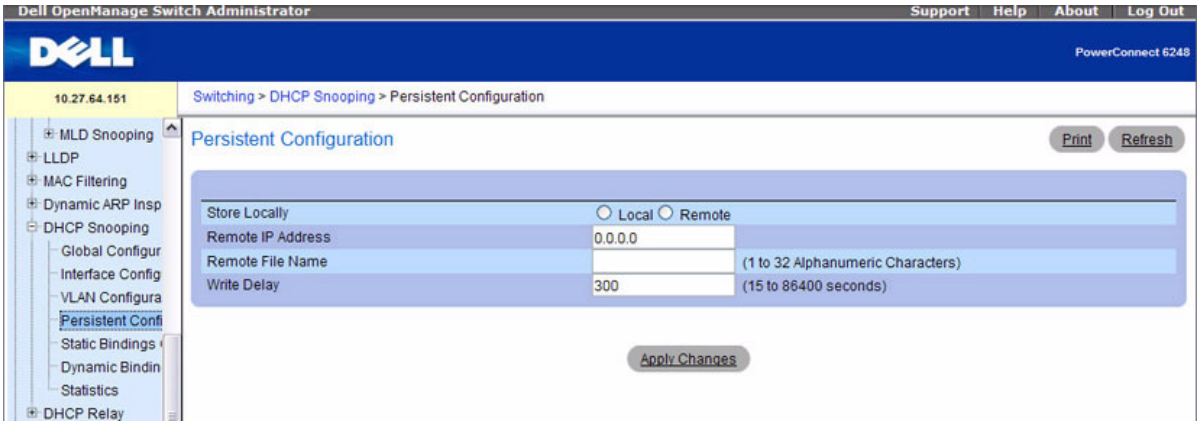
- DHCP Snooping Commands

DHCP Snooping Persistent Configuration

Use the **DHCP Snooping Persistent Configuration** page to configure the persistent location of the DHCP snooping database. This location can be local or remote on a given IP machine. For more information about DHCP bindings and the DHCP Snooping database, see "DHCP Snooping Static Bindings Configuration" on page 401.

To access the **DHCP Snooping Persistent Configuration** page, click **Switching > DHCP Snooping > Persistent Configuration** in the navigation tree.

Figure 7-114. DHCP Snooping Persistent Configuration



The **DHCP Snooping Persistent Configuration** page contains the following fields:

- **Store Locally** — Choose whether to store the DHCP snooping database locally in flash or on a remote system:

Downloaded from www.Manualslib.com manuals search engine

- **Local** — Select the Local check box to store the DHCP binding database in the flash memory on the switch.
- **Remote** — Check the Remote check box to store the DHCP binding database on a remote server.

- **Remote IP Address** — Enter the Remote IP address on which the snooping database will be stored when the Remote check box is selected.
- **Remote File Name** — Enter the Remote filename to store the database when the Remote check box is selected.
- **Write Delay** — Enter the maximum write time to write the database into the local or remote location. The write delay range is 15 to 86400 seconds.

Configuring DHCP Snooping With CLI Commands

For information about the CLI commands that perform this function, refer to the following chapter in the *CLI Reference Guide*:

- DHCP Snooping Commands

DHCP Snooping Static Bindings Configuration

Use the **DHCP Snooping Static Bindings Configuration** page to add static DHCP bindings to the binding database.

The DHCP snooping application uses DHCP messages to build and maintain the binding's database. The binding's database only includes data for clients on untrusted ports. DHCP snooping creates a tentative binding from DHCP DISCOVER and REQUEST messages. Tentative bindings tie a client to a port (the port where the DHCP client message was received). Tentative bindings are completed when DHCP snooping learns the client's IP address from a DHCP ACK message on a trusted port. DHCP snooping removes bindings in response to DECLINE, RELEASE, and NACK messages. The DHCP snooping application ignores the ACK messages as a reply to the DHCP Inform messages received on trusted ports. You can also enter static bindings into the binding database.

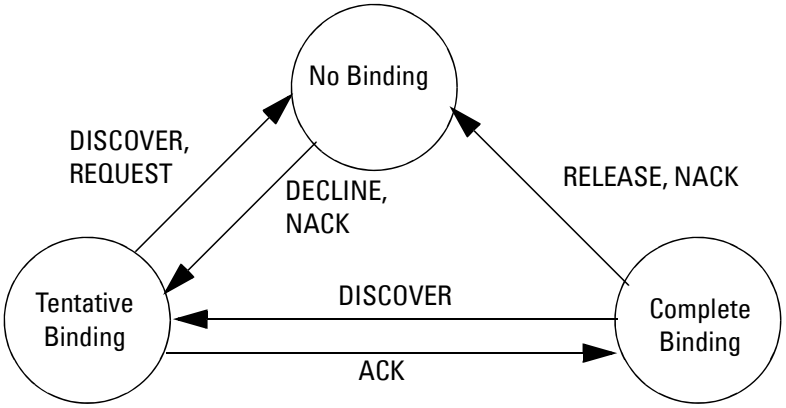
The DHCP binding database is persisted on a configured external server or locally in flash, depending on the user configuration. A row-wise checksum is placed in the text file that is going to be stored in the remote configured server. On reloading, the switch reads the configured binding file to build the DHCP snooping database. When the switch starts and the calculated checksum value equals the stored checksum, the switch reads entries from the binding file and populates the binding database. A checksum failure or a connection problem to the external configured server will cause the switch to loose the bindings and will cause a host's data loss if DAI is enabled.

When a switch learns of new bindings or when it loses bindings, the switch immediately updates the entries in the database. The switch also updates the entries in the binding file. The frequency at which the file is updated is based on a configurable delay, and the updates are batched.

Downloaded from www.Manualslib.com manuals search engine

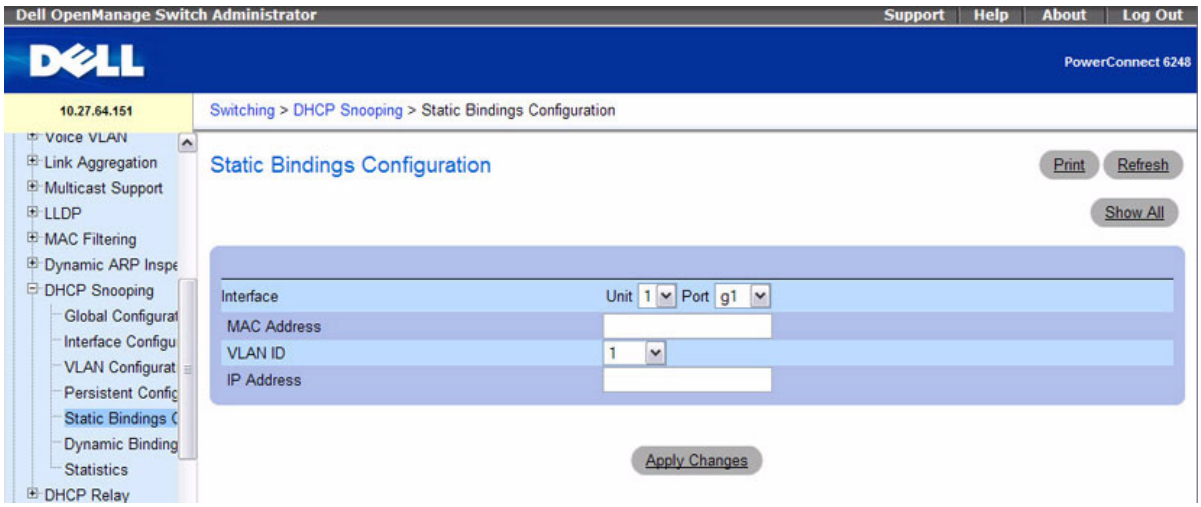
If the absolute lease time of the snooping database entry expires, then that entry will be removed. You should take care of the system time to be consistent across the reboots. Otherwise, the snooping entries will not expire properly. If a host sends a DHCP release while the switch is rebooting then, when the switch receives the DHCP discovery or request, the client's binding will go to the tentative binding as shown in the following figure.

Figure 7-115. States of Client Binding



To access the **DHCP Snooping Static Bindings Configuration** page, click **Switching > DHCP Snooping > Static Bindings Configuration** in the navigation tree.

Figure 7-116. DHCP Snooping Static Bindings Configuration



The **DHCP Snooping Static Bindings Configuration** page contains the following fields:

- **Interface** — Select the interface to add a binding into the DHCP snooping database.

Downloaded from www.Manualslib.com manuals search engine

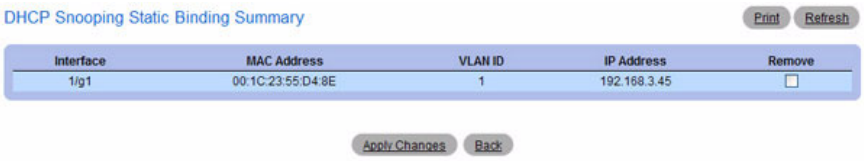
- **MAC Address** — Specify the MAC address for the binding to be added. This is the Key to the binding database.
- **VLAN ID** — Select the VLAN from the list for the binding rule. The range of the VLAN ID is 1 to 4093.
- **IP Address** — Specify a valid IP address for the binding rule.

Displaying the DHCP Snooping Static Bindings Summary Table

1. Open the **DHCP Snooping Static Bindings Configuration** page.
2. Click **Show All**.

   The **DHCP Snooping Static Bindings Summary** table displays.

Figure 7-117. DHCP Snooping Static Bindings Summary



Configuring DHCP Snooping With CLI Commands

For information about the CLI commands that perform this function, refer to the following chapter in the *CLI Reference Guide*:

- DHCP Snooping Commands

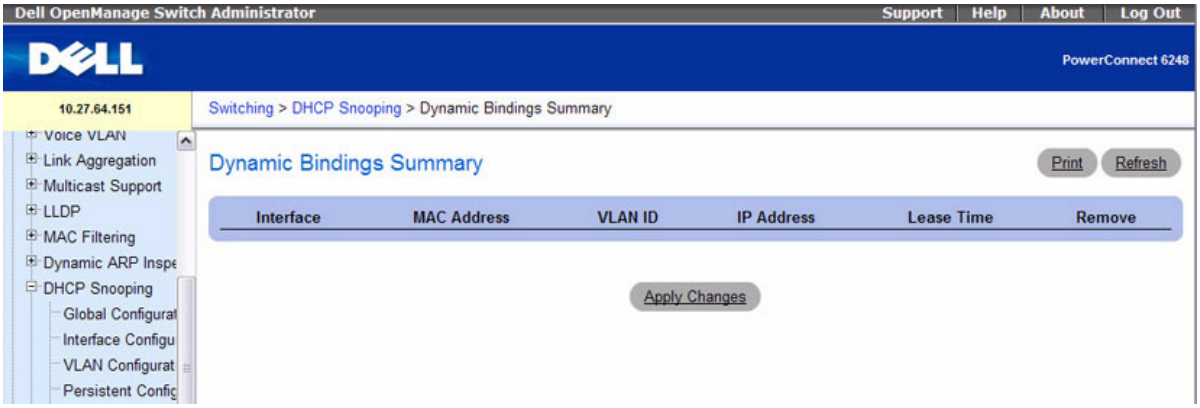
DHCP Snooping Dynamic Bindings Summary

The **DHCP Snooping Dynamic Bindings Summary** lists all the DHCP snooping dynamic binding entries learned on the switch ports.

To access the DHCP Snooping Dynamic Bindings Summary page, click **Switching > DHCP Snooping > Dynamic Bindings Summary** in the navigation tree.

Downloaded from www.Manualslib.com manuals search engine

Figure 7-118. DHCP Snooping Dynamic Bindings Summary



The **DHCP Snooping Dynamic Bindings Summary** page contains the following fields:

- **Interface** — Displays the interface.
- **MAC Address** — Displays the MAC address.
- **VLAN ID** — Displays the VLAN ID.
- **IP Address** — Displays the IP address.
- **Lease Time** — Displays the remaining Lease time for the dynamic entries.
- **Remove** — Select to remove the particular binding entry.

Viewing DHCP Snooping Information With CLI Commands

For information about the CLI commands that perform this function, refer to the following chapter in the *CLI Reference Guide*:

- DHCP Snooping Commands

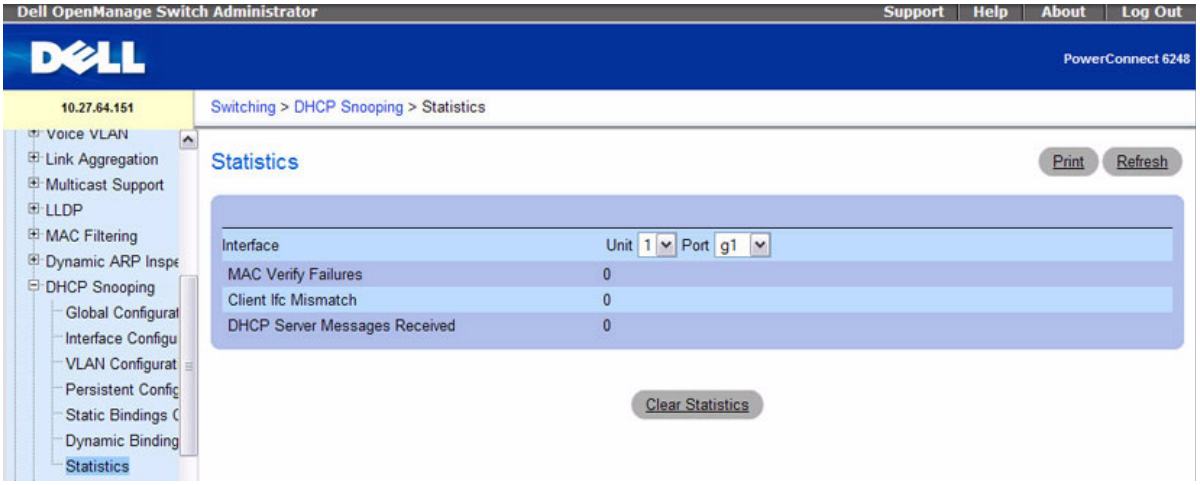
Downloaded from www.Manualslib.com manuals search engine

DHCP Snooping Statistics

The **DHCP Snooping Statistics** page displays DHCP snooping interface statistics.

To access the DHCP Snooping Statistics page, click **Switching > DHCP Snooping > Statistics** in the navigation tree.

Figure 7-119. DHCP Snooping Statistics



The **DHCP Snooping Statistics** page contains the following fields:

- **Interface** — Select the untrusted and snooping-enabled interface for which statistics are to be displayed.
- **MAC Verify Failures** — The number of packets that were dropped by DHCP snooping because there is no matching DHCP snooping binding entry found.
- **Client Ifc Mismatch** — The number of DHCP messages that are dropped based on the source MAC address and client hardware address verification.
- **DHCP Server Msgs Received** — The number of server messages that are dropped on an untrusted port.

Viewing DHCP Snooping Information With CLI Commands

For information about the CLI commands that perform this function, refer to the following chapter in the *CLI Reference Guide*:

- DHCP Snooping Commands

Downloaded from www.Manualslib.com manuals search engine

IP Source Guard

IP source guard (IPSG) is a security feature that filters IP packets based on source ID. The source ID may either be source IP address or a {source IP address, source MAC address} pair. IPSG is disabled by default.

NOTE: The PowerConnect 6220 does not support IPSG.

The **IP Source Guard** menu page contains links to the following features:

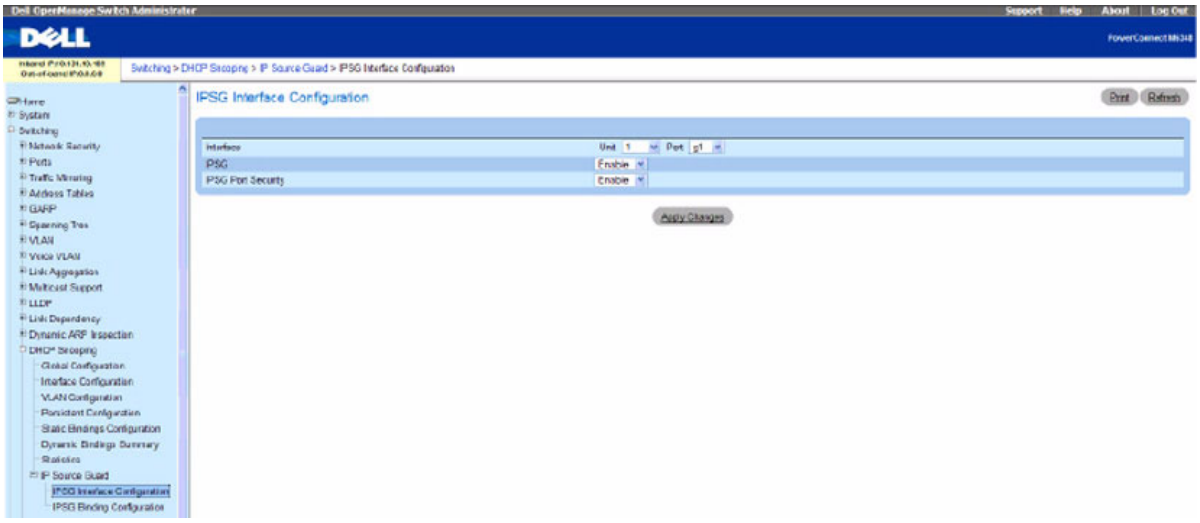
- IPSG Interface Configuration
- IPSG Binding Configuration
- IPSG Binding Configuration Summary

IPSG Interface Configuration

Use the IPSG Interface Configuration page to configure IPSG on an interface.

To access the IPSG Interface Configuration page, click **Switching > DHCP Snooping > IP Source Guard > IPSG Interface Configuration** in the navigation tree.

Figure 7-120. IPSG Interface Configuration



The **IPSG Interface Configuration** page contains the following fields:

- **Interface** — Select the interface on which IPSG is to be configured.
- **IPSG** — When enabled, drops all IP packets except the packets that match the source IP of any entry in the IPSG bindings table (irrespective of source Mac address).
- **IPSG Port Security** — When enabled , considers source MAC address for filtering out IP packets.

NOTE: Once IPSG Port security is enabled, it cannot not be disabled without disabling IPSG and IPSG Port security, and reenabling IPSG.

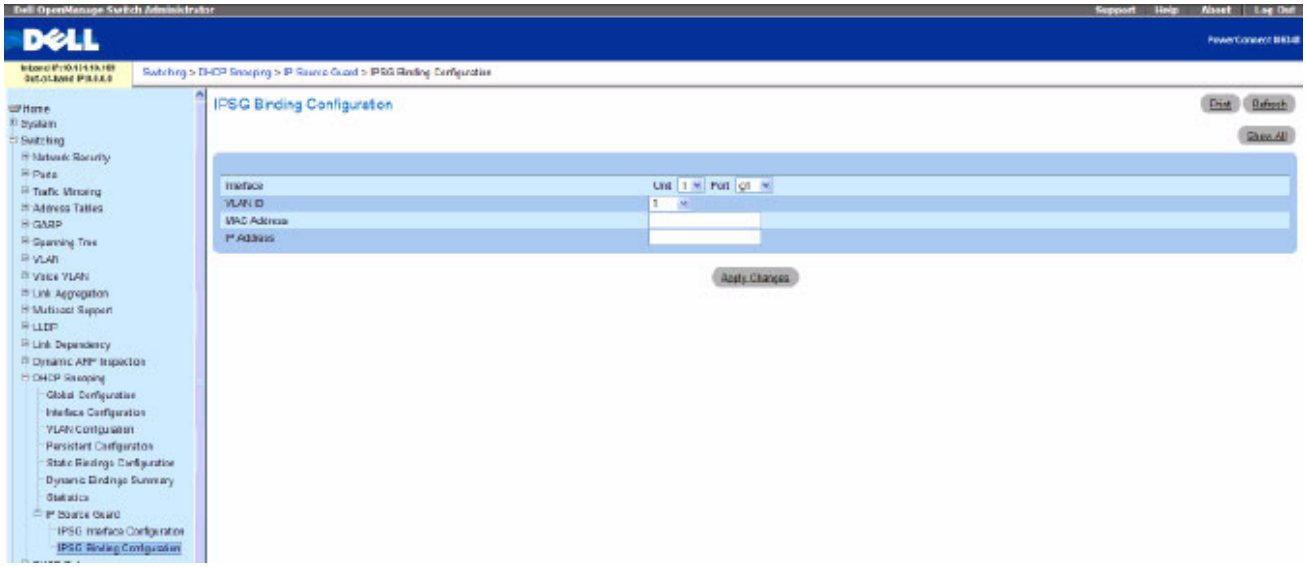
Downloaded from www.Manualslib.com manuals search engine

IPSG Binding Configuration

Use the **IPSG Binding Configuration** page displays DHCP snooping interface statistics.

To access the DHCP Snooping Statistics page, click **Switching > DHCP Snooping > IP Source Guard > IPSG Binding Configuration** in the navigation tree.

Figure 7-121. IPSG Binding Configuration



The **IPSG Binding Configuration** page contains the following fields:

- **Interface** — Select the interface on which IPSG binding is to be configured.
- **VLAN ID** — Specifies VLAN ID.
- **MAC Address** — Source Mac Address of the static IPSG binding.
- **IP Address** — Source IP address of the static IPSG binding.

Select the **Show All** button to open the IPGS Binding Configuration Summary page.

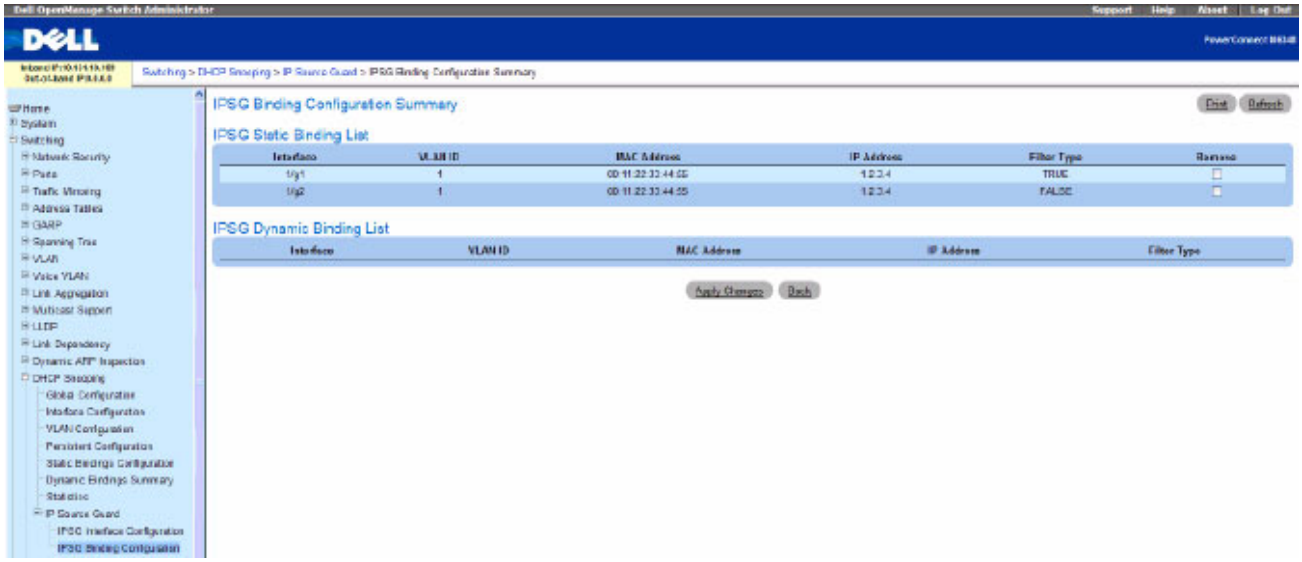
Downloaded from www.Manualslib.com manuals search engine

IPSG Binding Configuration Summary

The **IPSG Binding Configuration Summary** page displays the IPSG Static binding list and IPSG dynamic binding list (the static bindings configured in Binding configuration page).

To access the IPSG Binding Configuration Summary page, click **Switching > DHCP Snooping > IP Source Guard > IPSG Binding Configuration Summary** in the navigation tree.

Figure 7-122. IPSG Binding Configuration Summary



The **IPSG Binding Configuration Summary** page contains the following fields:

To remove an interface from the IPSG Binding list, select the **Remove** checkbox and select **Apply Changes**.

DHCP Relay

When a DHCP client and server are in the same IP subnet, they can directly connect to exchange IP address requests and replies. However, having a DHCP server on each subnet can be expensive and is often impractical. Alternatively, network infrastructure devices can be used to relay packets between a DHCP client and server on different subnets. Such a device, a Layer 3 Relay agent, is generally a router that has IP interfaces on both the client and server subnets and can route between them. However, in Layer 2 switched networks, there may be one or more infrastructure devices (for example, a switch) between the client and the L3 Relay agent/DHCP server. In this instance, some of the client device information required by the L3 Relay agent may not be visible to it. In this case, an L2 Relay agent can be used to add the information that the L3 Relay Agent and DHCP server need to perform their roles in address and configuration and assignment.

Downloaded from www.Manualslib.com manuals search engine

Before it relays DHCP requests from clients, the switch can add a Circuit ID and a Remote ID. These provide information about the circuit and port number connected to the client. This information is added as suboptions in the DHCP Option 82 packets (see sections 3.1 and 3.2 of RFC3046). The switch removes this option from packets that it relays from L3 Relay agents/DHCP servers to clients.

These sub-options may be used by the DHCP server to affect how it treats the client, and also may be used by the relay agent to limit broadcast replies to the specific circuit or attachment point of the client.

The **Switching > DHCP Relay** page provides links to the following pages:

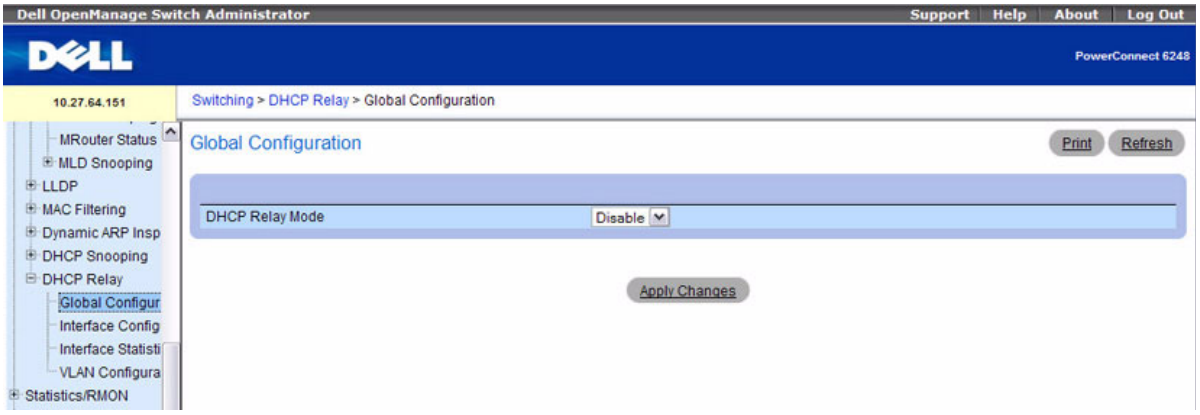
- DHCP Relay Global Configuration
- DHCP Relay Interface Configuration
- DHCP Relay Interface Statistics
- DHCP Relay VLAN Configuration

DHCP Relay Global Configuration

Use this page to enable or disable the switch to act as a DHCP Relay agent. This functionality must also be enabled on each port you want this service to operate on (see DHCP Relay Interface Configuration). The switch can also be configured to relay requests only when the VLAN of the requesting client corresponds to a service provider's VLAN ID that has been enabled with the L2 DHCP relay functionality (see DHCP Relay VLAN Configuration).

To access this page, click **Switching > DHCP Relay > Global Configuration** in the tree view.

Figure 7-123. DHCP Relay Global Configuration



If you enable or disable the **DHCP Relay** feature, click **Apply Changes** to submit the changes to system.

Configuring DHCP Relay With CLI Commands

For information about the CLI commands that perform this function, refer to the following chapter in the *CLI Reference Guide*:

- L2 DHCP Relay Agent Commands

Downloaded from www.Manualslib.com manuals search engine

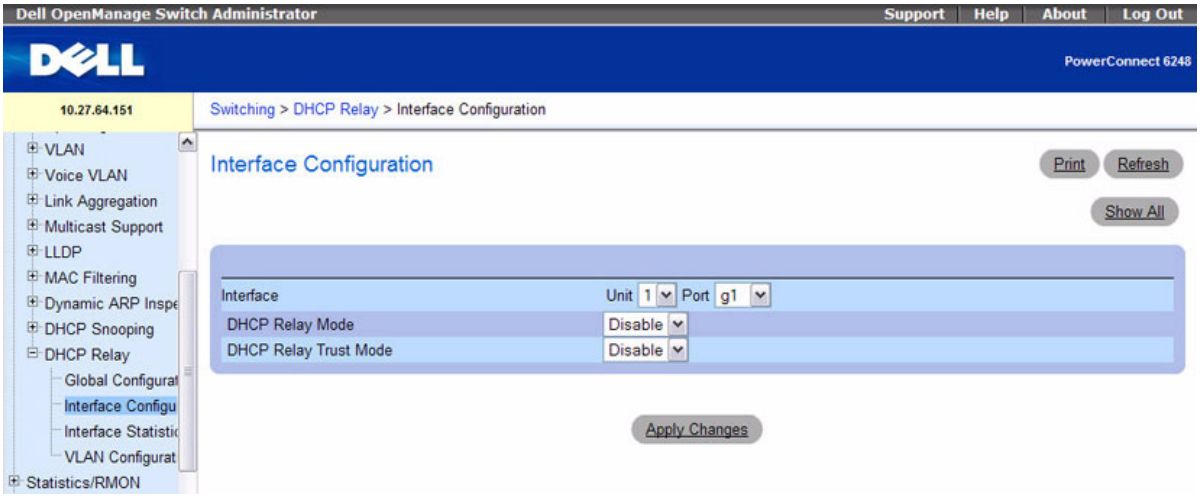
DHCP Relay Interface Configuration

Use this page to enable L2 DHCP relay on individual ports.

NOTE: L2 DHCP relay must also be enabled globally on the switch.

To access this page, click **Switching** > **DHCP Relay** > **Interface Configuration** in the tree view.

Figure 7-124. DHCP Relay Interface Configuration



The **DHCP Relay Interface Configuration** page contains the following fields:

- **Interface** — Select the slot/port to configure this feature on.
- **DHCP Relay Mode** — Enable or disable L2 Relay mode on the selected interface.
- **DHCP Relay Trust Mode** — Enable or disable L2 Relay Trust Mode on the selected interface.

  Trusted interfaces usually connect to other agents or servers participating in the DHCP interaction (e.g. other L2 or L3 Relay Agents or Servers). When enabled in Trust Mode, the interface always expects to receive DHCP packets that include Option 82 information. If Option 82 information is not included, then these packets are discarded.

  Untrusted interfaces are generally connected to clients. DHCP packets arriving on an untrusted interface are never expected to carry Option 82 and are discarded if they do.

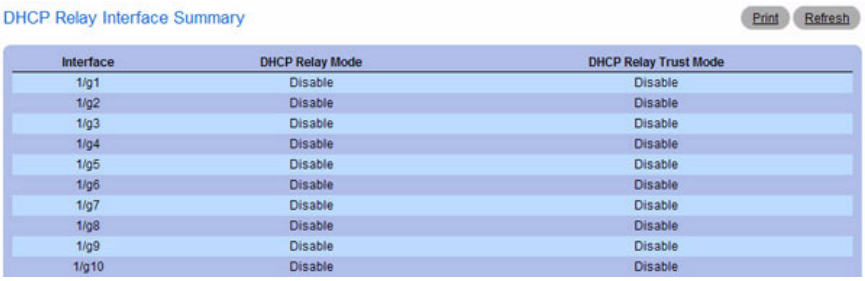
Displaying the DHCP Relay Interface Summary Table

1. Open the **DHCP Relay Interface Configuration** page.
2. Click **Show All**.

   The **DHCP Relay Interface Summary** table displays.

Downloaded from www.Manualslib.com manuals search engine

Figure 7-125. DHCP Relay Interface Summary



Interface	DHCP Relay Mode	DHCP Relay Trust Mode
1/g1	Disable	Disable
1/g2	Disable	Disable
1/g3	Disable	Disable
1/g4	Disable	Disable
1/g5	Disable	Disable
1/g6	Disable	Disable
1/g7	Disable	Disable
1/g8	Disable	Disable
1/g9	Disable	Disable
1/g10	Disable	Disable

Configuring DHCP Relay With CLI Commands

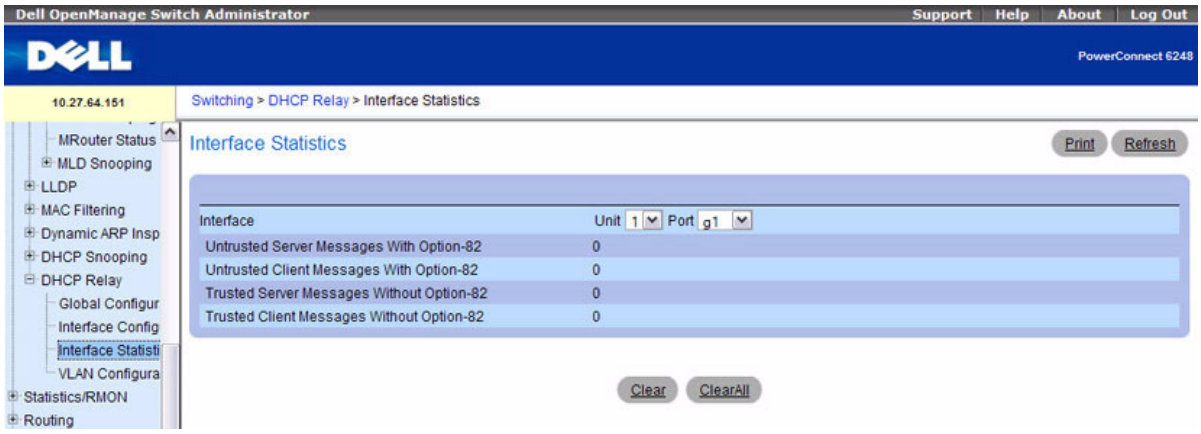
For information about the CLI commands that perform this function, refer to the following chapter in the *CLI Reference Guide*:

- L2 DHCP Relay Agent Commands

DHCP Relay Interface Statistics

Use this page to display statistics on DHCP Relay requests received on a selected port. To access this page, click **Switching > DHCP Relay > Interface Statistics** in the tree view.

Figure 7-126. DHCP Relay Interface Statistics



Downloaded from www.Manualslib.com manuals search engine

The **DHCP Relay Interface Statistics** page contains the following fields:

- **Interface** — Select the slot/port to configure this feature on.
- **Untrusted Server Msgs With Option-82** — If the selected interface is configured in untrusted mode, this field shows the number of messages received on the interface from a DHCP server that contained Option 82 data.These messages are dropped.
- **Untrusted Client Msgs With Option-82** — If the selected interface is configured in untrusted mode, this field shows the number of messages received on the interface from a DHCP client that contained Option 82 data.These messages are dropped.
- **Trusted Server Msgs Without Option-82** — If the selected interface is configured in trusted mode, this field shows the number of messages received on the interface from a DHCP server that did not contain Option 82 data. These messages are dropped.
- **Trusted Client Msgs Without Option-82** — If the selected interface is configured in trusted mode, this field shows the number of messages received on the interface from a DHCP client that did not contain Option 82 data. These messages are dropped.

Use the buttons on the page to perform the following:

- Click **Clear** to set statistics for this port to their initial values.
- Click **Clear All** to set statistics for all ports to their initial values.

Viewing DHCP Relay Information With CLI Commands

For information about the CLI commands that perform this function, refer to the following chapter in the *CLI Reference Guide*:

- L2 DHCP Relay Agent Commands

Downloaded from www.Manualslib.com manuals search engine

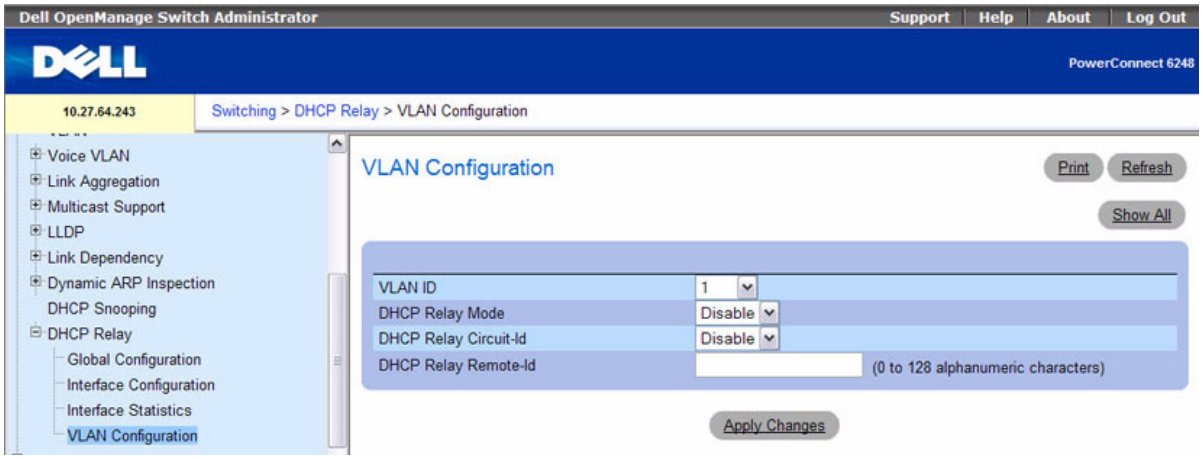
DHCP Relay VLAN Configuration

You can enable L2 DHCP relay on a particular VLAN. The VLAN is identified by a service VLAN ID (S-VID), which a service provider uses to identify a customer's traffic while traversing the provider network to multiple remote sites. The switch uses the VLAN membership of the switch port client (the customer VLAN ID, or C-VID) to perform a lookup a corresponding S-VID.

If the S-VID is enabled for DHCP Relay, then the packet can be forwarded. If the C-VID does not correspond to an S-VID that is enabled for DHCP Relay, then the switch will not relay the DHCP request packet.

To access this page, click **Switching > DHCP Relay > VLAN Configuration** in the tree view.

Figure 7-127. DHCP Relay VLAN Configuration



The **DHCP Relay VLAN Configuration** page contains the following fields:

- **VLAN ID** — Select a VLAN ID from the list for configuration. This is an S-VID (as indicated by the service provider) that identifies a VLAN that is authorized to relay DHCP packets through the provider network.
- **DHCP Relay Mode** — Enable or disable the selected VLAN for DHCP Relay services. The default is **Disable**.
- **DHCP Relay Circuit-Id** — When enabled, if a client sends a DHCP request to the switch and the client is in a VLAN that corresponds to the selected S-VID, the switch adds the client's interface number to the Circuit ID sub-option of Option 82 in the DHCP request packet. The default is **Disable**.

  This enables the switch to reduce the broadcast domain to which the server replies are switched when the broadcast bit is set for DHCP packets. When this bit is set, the server is required to echo the Option-82 in replies. Since the circuit-id field contains the client interface number, the L2 relay agent can forward the response to the requesting interface only, rather to all ports in the VLAN).

Downloaded from www.Manualslib.com manuals search engine

- **DHCP Relay Remote-Id** — When a string is entered here, if a client sends a DHCP request to the switch and the client is in a VLAN that corresponds to the selected S-VID, then the switch adds the string to the Remote-ID sub-option of Option 82 in the DHCP request packet. The range is 0-128 alphanumeric characters. The default is **NULL** string.

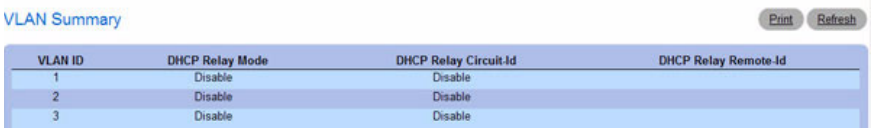
  This sub-option can be used by the server for parameter assignment. The content of this option is vendor-specific.

Displaying the DHCP Relay VLAN Summary Table

1. Open the **DHCP Relay VLAN Configuration** page.
2. Click **Show All**.

   The **DHCP Relay VLAN Summary** table displays.

Figure 7-128. DHCP Relay VLAN Summary



VLAN ID	DHCP Relay Mode	DHCP Relay Circuit-Id	DHCP Relay Remote-Id
1	Disable	Disable	
2	Disable	Disable	
3	Disable	Disable	

Configuring DHCP Relay With CLI Commands

For information about the CLI commands that perform this function, refer to the following chapter in the *CLI Reference Guide*:

L2 DHCP Relay Agent Commands

Using the Port Aggregator Feature

The Port Aggregator feature minimizes the administration required for managing the blade-centric switch blades. This feature provides administrators the ability to map internal ports to external ports without having to know anything about STP, VLANs, Link Aggregation or other L2/L3 protocols.

The Port Aggregator feature is only available when the switch is operating in Simple mode, which is disabled by default. For information about changing the mode, see "Setting the Operational Mode" on page 130.

To display the **Port Aggregator** page, click **Switching > Port Aggregator** in the tree view. Use this page to go to the following features:

- Port Configuration Summary
- Group Configuration Summary
- Group VLAN MAC Summary

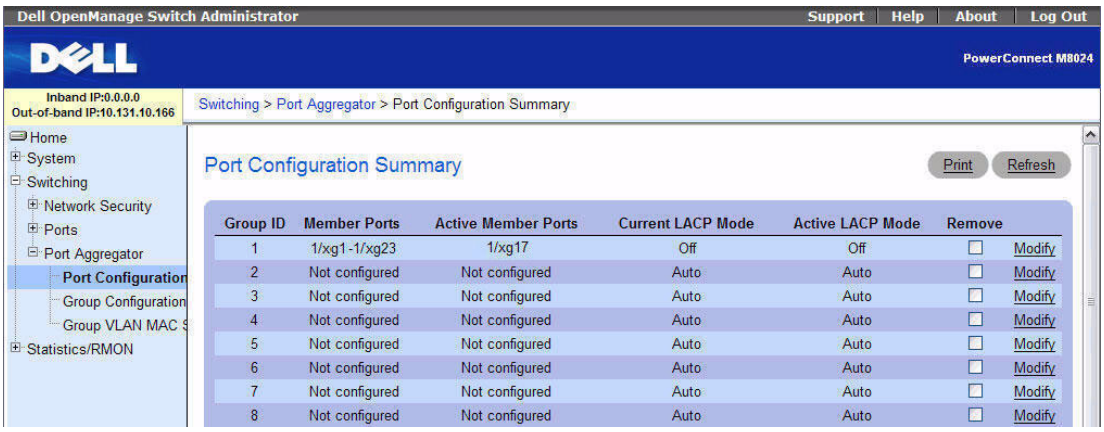
Downloaded from www.Manualslib.com manuals search engine

Port Configuration Summary

Use the **Port Configuration Summary** page to view information about the port members and LACP modes for the aggregator groups. From the **Port Configuration Summary** page, you can access the **Port Configuration** page.

To display the **Port Configuration Summary** page, click **Switching > Port Aggregator > Port Configuration Summary** in the tree view.

Figure 7-129. Port Configuration Summary



The **Port Configuration Summary** page contains the following fields:

- **Group ID** — Lists the ID for the aggregator group. The group ID range is 1–8. For switches that are not in a stack, the group ID range is 1–8. For stacked switches, the group ID range is 1–72.
- **Member Ports** — Identifies which ports are members of the group. By default, all ports are members of Group 1.
- **Active Member Ports—**Indicates which ports within the aggregator group have an active link. The link is active (UP) when the port is administratively enabled and operational.
- **Current LACP Mode** — Displays the LACP mode configured on the port, which can be Auto, Static, or Off.
- **Active LACP Mode —** Displays the LACP mode that the group is currently operating in, which might be different than the Current LACP Mode depending on the partner switch.

Downloaded from www.Manualslib.com manuals search engine

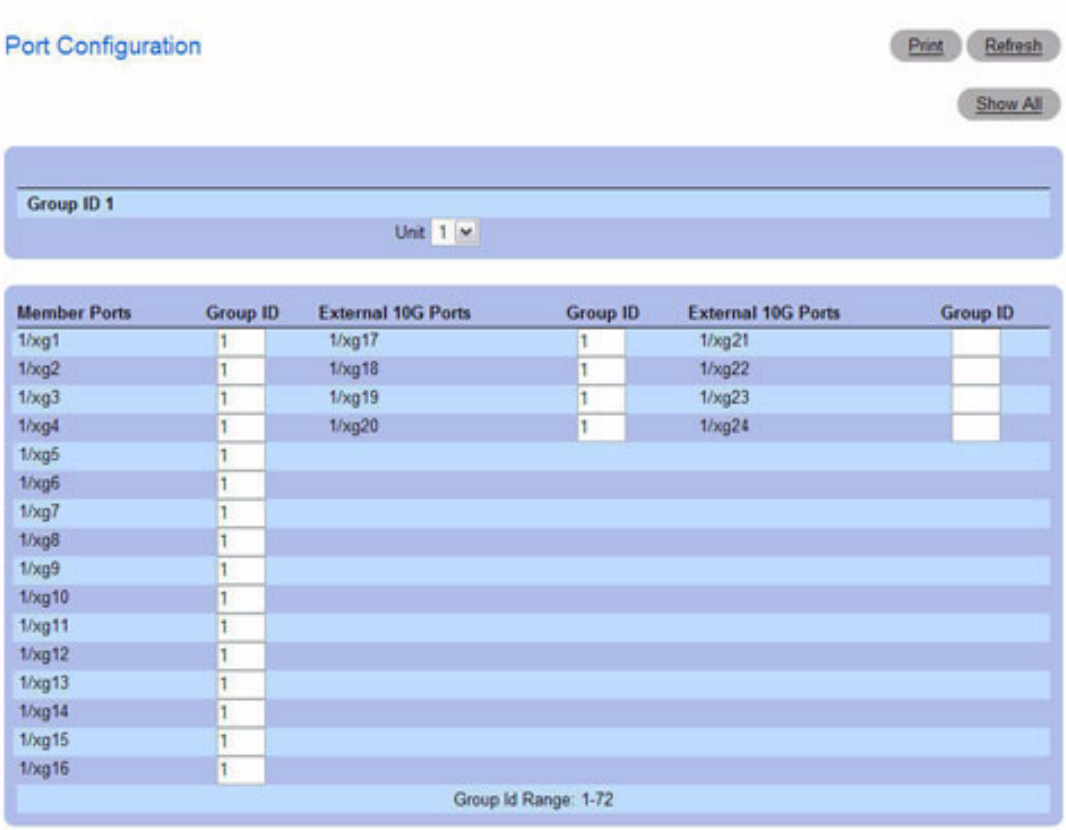
Configuring Port Aggregator Groups

You can assign each port to an aggregator group from the **Port Configuration** page, which is accessible from the **Port Configuration Summary** page. By default, all ports are in aggregator group 1.

1. Open the **Port Configuration Summary** page.
2. Click any **Modify** link to access the **Port Configuration** page.

   The **Port Configuration** page displays.

Figure 7-130. Port Aggregator Group Port Configuration



3. If the system supports stacking, select the stack member to configure.
4. Enter the Port Aggregator Group ID in the Group ID field for the ports to add to a group.

   Each port can only belong to one Port Aggregator group.
5. Click **Apply Changes**.
6. To return to the **Port Configuration Summary** page, click **Show All**.

Downloaded from www.Manualslib.com manuals search engine

Removing Ports from an Aggregator Group

1. Open the **Port Configuration Summary** page.
2. Select the **Remove** option for the group with the ports to remove.
3. Click **Apply Changes**.

   All ports assigned to the Port Aggregator group are removed from the group and are not assigned to any group.

   Note: To delete a single port from a group, click **Modify** to access the **Port Configuration** page, delete the group ID from the port's Group ID field, and then click **Apply Changes**.

Configuring Port Configuration Settings with CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

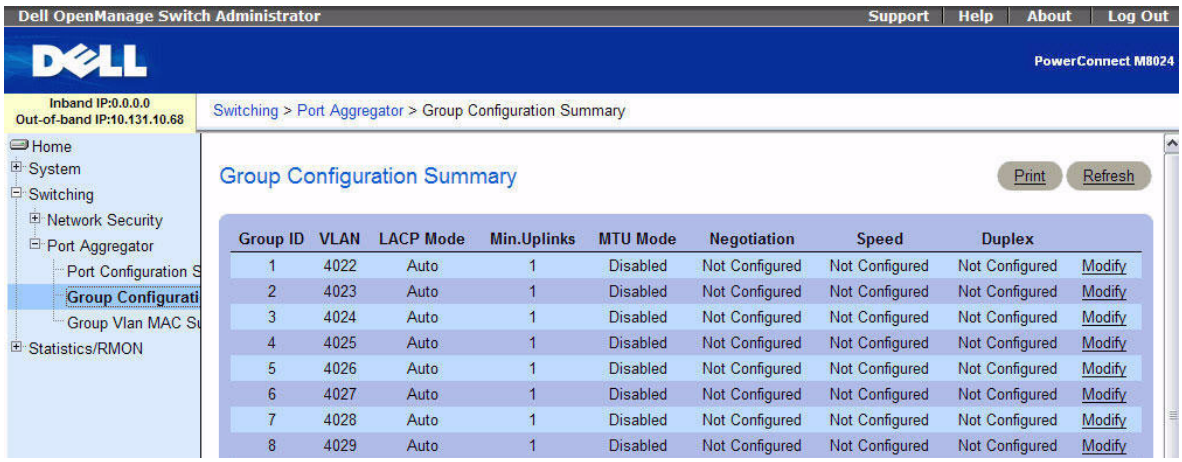
- Port Aggregator Commands

Group Configuration Summary

Use the **Group Configuration Summary** page to view information about the port aggregator group configuration for all groups. From the **Group Configuration Summary** page, you can access the **Group Configuration** page for each group and change the group settings.

To display the **Group Configuration Summary** page, click **Switching > Port Aggregator > Group Configuration Summary** in the tree view.

Figure 7-131. Group Configuration Summary



Downloaded from www.Manualslib.com manuals search engine

The **Group Configuration Summary** page contains the following fields:

- **Group ID** — Identifies the aggregator group.
- **VLAN** — Select the VLAN or VLANs that will have the Aggregator Group as a member. An Aggregator Group can be a member of multiple VLANs, but each VLAN can only belong to one Aggregator Group. By default, a VLAN is reserved for each group, starting with VLAN 4022 for group 1. The reserved VLAN cannot be deleted from the group, but you can configure the group to participate in additional unreserved VLANs.
- **LACP Mode —** Identifies the LACP mode for the aggregator group. The available options are Auto, Static, or Off:
  - **Auto** — External ports are automatically configured as a LACP trunk group. External switches must support LACP if multiple external ports are members of this Aggregator Group. Uplink ports in the Aggregator Group receive LACP PDUs, listen for the LACPDUs from the partner, and negotiate the Link Aggregation. External (uplink) ports will be re-enabled once LACP is detected on the active uplink without user intervention.
  - Static — The uplink ports in the Aggregator Group are set to Static mode. Static LAGs are recommended when connecting the PowerConnect M6220/M6348/M8024 switch to an external Ethernet switch that does not support LACP.
  - **Off** — Link Aggregation is off, and the aggregator group has only one uplink port. This mode avoids any possible loops in the network.
- **Min. Uplinks** — Identifies the minimum number of external (uplink) ports to be active in order for the Aggregation Group to be active. For example, when a switch has two external ports in the group and four internal ports, if the minimum active uplink ports is two, then both external ports must be active; otherwise, all the internal ports in the aggregator group will be brought DOWN. By default, the minimum active uplinks for an Aggregator Group is 1, which means at least one uplink port should be active for the Aggregator Group to be active.
- **MTU Mode** — Shows whether support for jumbo frames is enabled or disabled. Jumbo frames enables transporting identical data in fewer frames to ensure less overhead, lower processing time, and fewer interrupts.
- **Negotiation** — Shows whether Auto Negotiation is enabled or disabled on the group. Auto Negotiation is a protocol between two link partners that enables a port to advertise its transmission rate, duplex mode and flow control abilities to its partner.
- **Speed** — Identifies the port speed to be advertised by the ports in the group. If the speed is not supported by a port in the group, the port will ignore the speed and transmit data at the last successful speed setting. The possible field values are:
  - 10 — Indicates that the valid ports in the group advertise a 10 Mbps data rate.
  - 100 — Indicates that the valid ports in the group advertise a 100 Mbps data rate.
  - 1000 — Indicates that the valid ports in the group advertise a 1000 Mbps data rate.
  - 10000 — Indicates that the valid ports in the group advertise a 10000 Mbps data rate.

Downloaded from www.Manualslib.com manuals search engine

- **Duplex** — Identifies the group duplex mode, which is either Full or Half.
  - **Full** — Indicates that the group supports transmission between the switch and the client in both directions simultaneously.
  - **Half** — Indicates that the group supports transmission between the switch and the client in only one direction at a time.

Configuring a Port Aggregator Group

1. Open the **Group Configuration Summary** page.
2. For the group to configure, click the **Modify** link at the end of the row.

   The **Group Configuration** page for the group displays.

Figure 7-132. Group Configuration

3. Edit the fields as needed.

   For more information about the fields and the available options, see the field descriptions for the **Group Configuration Summary** page.
4. Click **Apply Changes**.

   The settings for the Port Aggregator group are modified, and the device is updated.
5. To return to the **Group Configuration Summary** page, click **Show All**.

Configuring Group Configuration Summary Settings with CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- Port Aggregator Commands

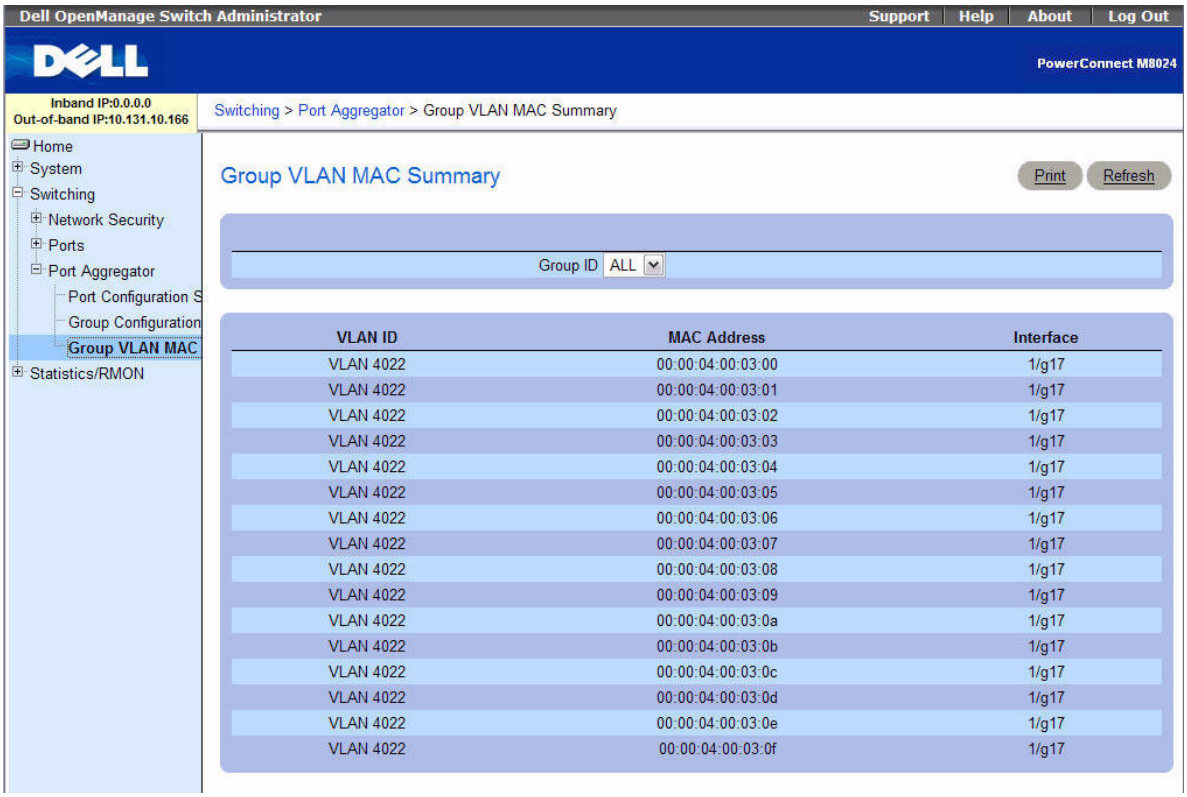
Downloaded from www.Manualslib.com manuals search engine

Group VLAN MAC Summary

Use the **Group VLAN MAC Summary** page to view the MAC address table entries for one Port Aggregator group or all groups.

To display the **Group VLAN MAC Summary** page, click **Switching > Port Aggregator > Group VLAN MAC Summary** in the tree view.

Figure 7-133. Group VLAN MAC Summary



The **Group VLAN MAC Summary** page contains the following fields:

- **Group ID** — Select the Port Aggregator group with the information to view. To view information for all groups, select All.
- **VLAN —** Identifies the VLAN on which the MAC address was learned.
- **MAC Address** — Identifies the MAC address that was learned on the VLAN.
- **Interface** — Identifies the port on which the MAC address was learned.

Viewing VLAN MAC Summary Information by using CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- Port Aggregator Commands

Downloaded from www.Manualslib.com manuals search engine

8

Viewing Statistics and Remote Monitoring

Overview

This section explains the RMON options available from the **Statistics/RMON** menu page. These options include viewing statistics in table form, editing and viewing RMON statistics, and charting Port and LAG statistics. The **Statistics/RMON** menu page provides access to these options through the following menu pages:

- Table Views
- RMON
- Charts

Note: CLI commands are not available for all the Statistics/RMON pages.

Remote Monitoring (RMON) allows the network administrator to get an idea of the network's performance and status through remote access. Four monitoring groups (defined as part of the RMON standard) are supported:

- Statistics
- History
- Alarms
- Events

Downloaded from www.Manualslib.com manuals search engine

Table Views

The **Table Views** menu page contains links to web pages that display statistics in table form. To display this page, click **Statistics/RMON > Table Views** in the tree view. Following are the web pages accessible from this menu page:

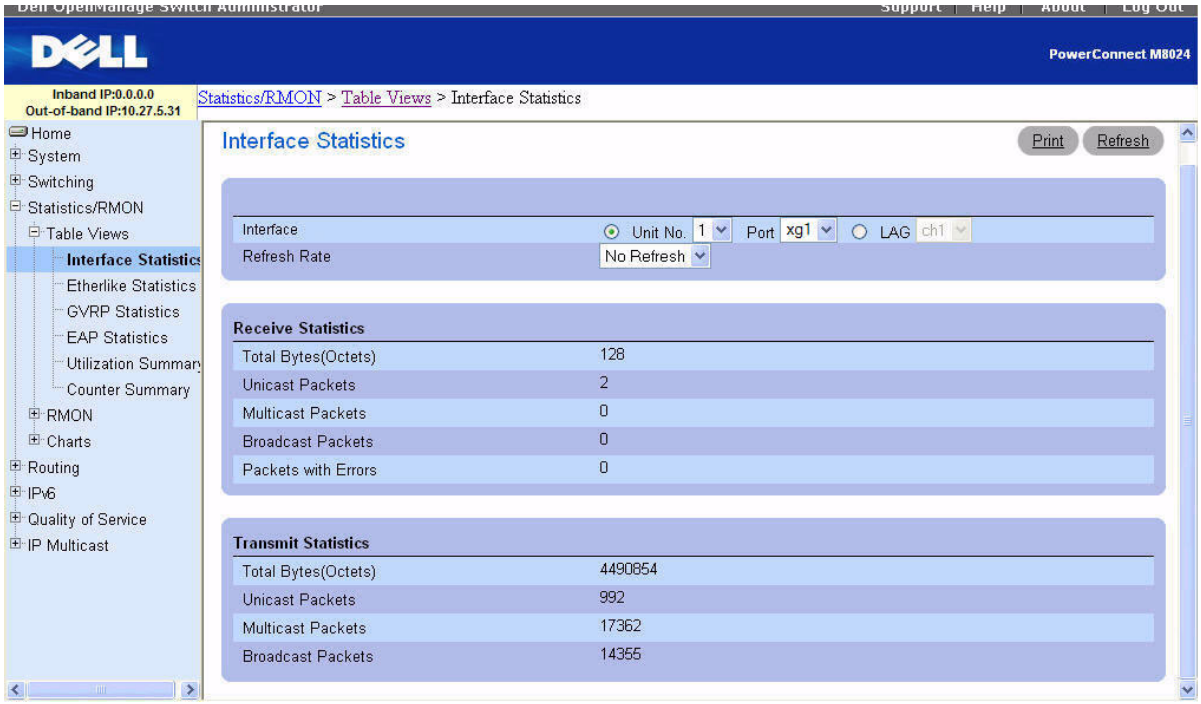
- Interface Statistics
- Etherlike Statistics
- GVRP Statistics
- EAP Statistics
- Utilization Summary
- Counter Summary

Interface Statistics

Use the **Interface Statistics** page to display statistics for both received and transmitted packets. The fields for both received and transmitted packets are identical.

To display the page, click **Statistics/RMON > Table Views > Interface Statistics** in the tree view.

Figure 8-1. Interface Statistics



Downloaded from www.Manualslib.com manuals search engine

The **Interface Statistics** page contains the following fields:

- **Interface** — Select physical interface (unit, port) or LAG interface for which statistics is displayed.
- **Refresh Rate** — Specifies amount of time that passes before statistics are refreshed. The possible field values are No Refresh, 15, 30 and 60 seconds. Default is No Refresh.

Received Statistics

- **Total Bytes (Octets)** — Displays the total number of octets received on the selected interface.
- **Unicast Packets** — Displays the total number of Unicast packets received on the selected interface.
- **Multicast Packets** — Displays the total number of Multicast packets received on the selected interface.
- **Broadcast Packets** — Displays the total number of Broadcast packets received on the selected interface.
- **Packets with Errors** — Displays the total number of packets with errors received on the selected interface.

Transmit Statistics

- **Total Bytes (Octets)** — Displays the total number of octets transmitted on the selected interface.
- **Unicast Packets** — Displays the total number of Unicast packets transmitted on the selected interface.
- **Multicast Packets** — Displays the total number of Multicast packets transmitted on the selected interface.
- **Broadcast Packets** — Displays the total number of Broadcast packets transmitted on the selected interface.

Displaying Interface Statistics

1. Open the **Interface Statistics** page.
2. Specify an interface.

   Statistics for specified interface display.

Viewing Interface Statistics Using the CLI Command

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- Ethernet Configuration Commands

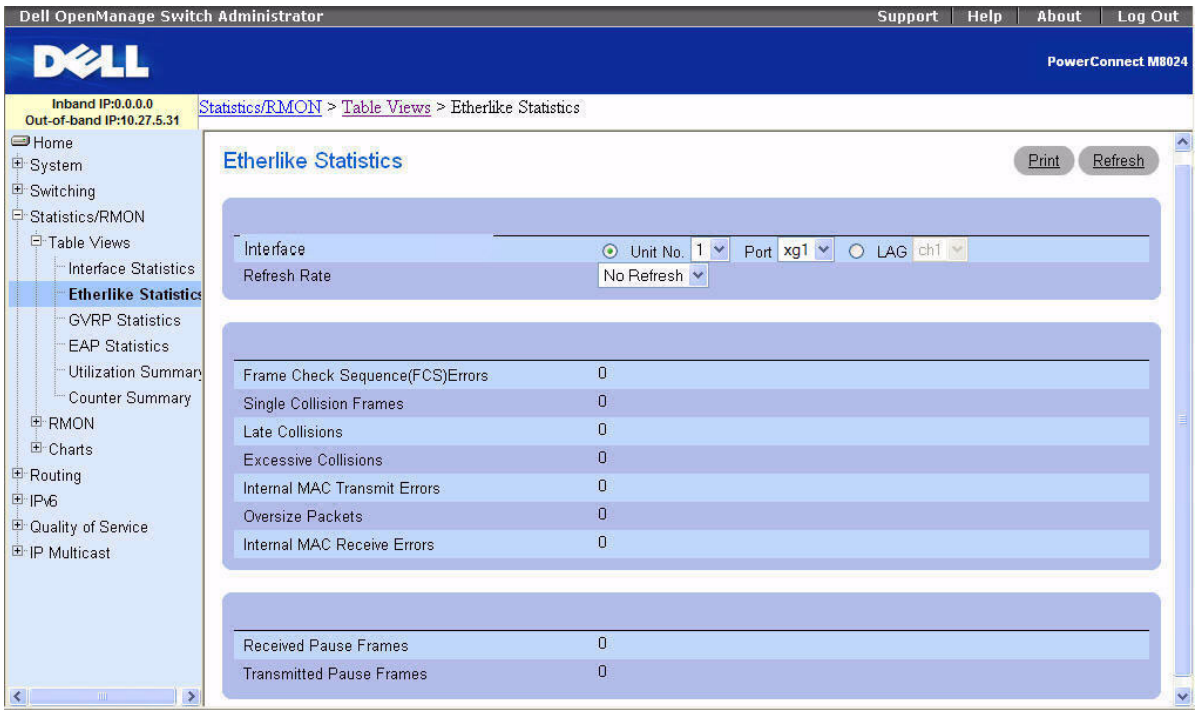
Downloaded from www.Manualslib.com manuals search engine

Etherlike Statistics

Use the **Etherlike Statistics** page to display interface statistics.

To display the page, click **Statistics/RMON > Table Views > Etherlike Statistics** in the tree view.

Figure 8-2. Etherlike Statistics



The **Etherlike Statistics** page contains the following fields:

- **Interface** — Select physical interface (unit, port) or LAG interface for which statistics is displayed.
- **Refresh Rate** — Specifies amount of time that passes before statistics are refreshed. The possible field values are No Refresh, 15, 30 and 60 seconds. Default is No Refresh.
- **Frame Check Sequence (FCS) Errors** — Displays number of FCS errors received on the selected interface.
- **Signal Collision Frames** — Displays number of signal collision frame errors received on the selected interface.
- **Late Collisions** — Displays number of late collisions received on the selected interface.
- **Excessive Collisions** — Displays number of excessive collisions received on the selected interface.
- **Internal MAC Transmit Errors** — Displays number of internal MAC transmit errors on the selected interface.
- **Oversize Packets** — Displays the total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.

Downloaded from www.Manualslib.com manuals search engine

- **Internal MAC Receive Errors** — Displays number of internal MAC received errors on the selected interface.
- **Received Pause Frames** — Displays number of received paused frames on the selected interface.

Transmitted Pause Frames — Displays number of transmitted paused frames on the selected interface.

Displaying Etherlike Statistics for an Interface

1. Open the **Etherlike Statistics** page.
2. Specify an interface.

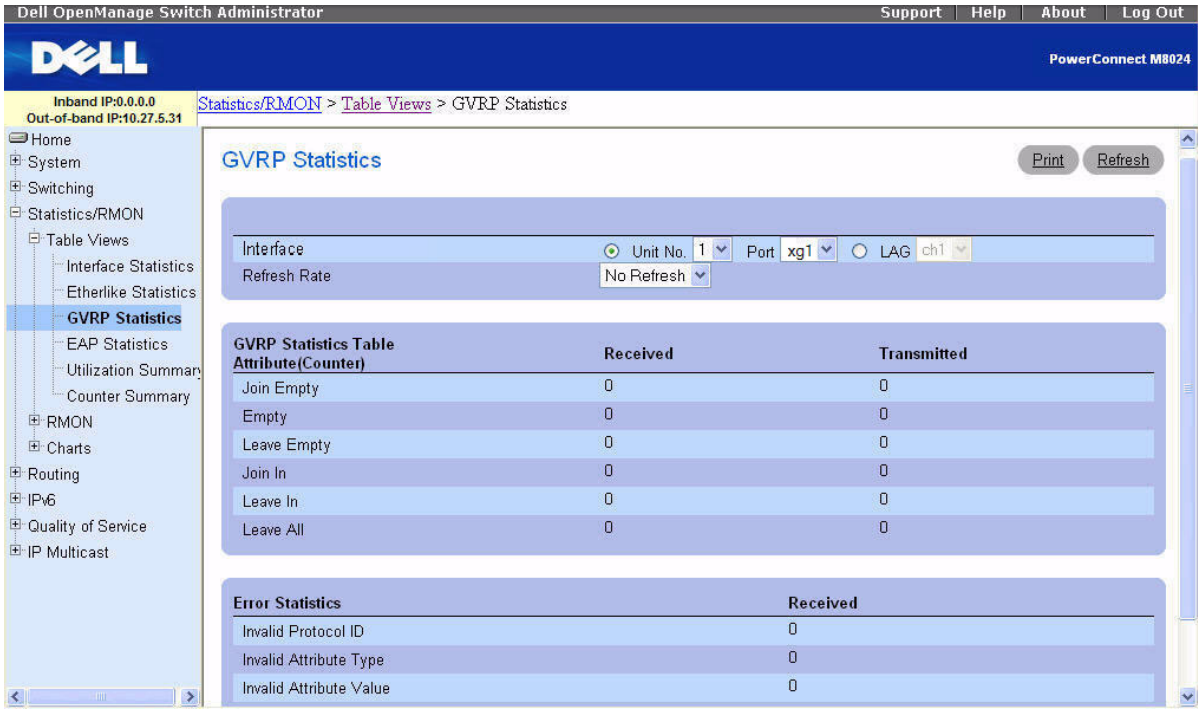
   Statistics for the specified interface display.

GVRP Statistics

Use the **GVRP Statistics** page to display switch statistics for GVRP.

To display the page, click **Statistics/RMON > Table Views > GVRP Statistics** in the tree view.

Figure 8-3. GVRP Statistics



Downloaded from www.Manualslib.com manuals search engine

The **GVRP Statistics** page contains the following fields:

- **Interface** — Select physical interface (unit, port) or LAG interface for which statistics will be displayed.
- **Refresh Rate** — Specifies amount of time that passes before statistics are refreshed. The possible field values are No Refresh, 15, 30, and 60 seconds. Default is No Refresh.

GVRP Statistics Table Attribute (Counters) - Received and Transmitted

- **Join Empty** — Displays switch GVRP Join Empty statistics.
- **Empty** — Displays switch GVRP Empty statistics.
- **Leave Empty** — Displays switch GVRP Leave Empty statistics.
- **Join In** — Displays switch GVRP Join In statistics.
- **Leave In** — Displays switch GVRP Leave In statistics.
- **Leave All** — Displays switch GVRP Leave All statistics.

Error Statistics - Received

- **Invalid Protocol ID** — Displays switch GVRP Invalid Protocol ID statistics.
- **Invalid Attribute Type** — Displays switch GVRP Invalid Attribute Type statistics.
- **Invalid Attribute Value** — Displays switch GVRP Invalid Attribute Value statistics.
- **Invalid Attribute Length** — Displays switch GVRP Invalid Attribute Length statistics.
- **Invalid Event** — Displays switch GVRP Invalid Event statistics.

Displaying GVRP Statistics for an Interface

1. Open the **GVRP Statistics** page.
2. Select an interface in the Interface field.

   GVRP Statistics display for the specified interface.

Viewing GVRP Statistics Using the CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- GVRP Commands

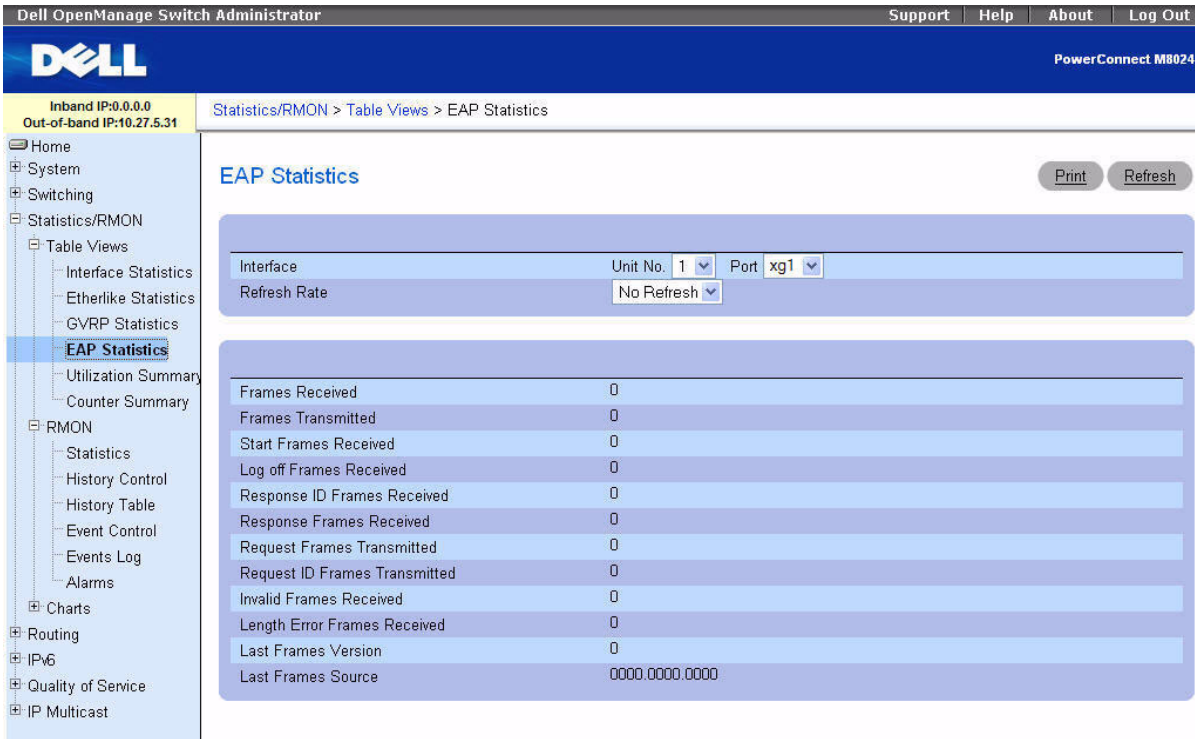
Downloaded from www.Manualslib.com manuals search engine

EAP Statistics

Use the **EAP Statistics** page to display information about EAP packets received on a specific port. For more information about EAP, see "Dot1x Authentication."

To display the **EAP Statistics** page, click **Statistics/RMON** > **Table Views** > **EAP Statistics** in the tree view.

Figure 8-4. EAP Statistics



The **EAP Statistics** page contains the following fields:

- **Interface** — Specifies the interface which is polled for statistics.
- **Refresh Rate** — Specifies amount of time that passes before statistics are refreshed. The possible field values are No Refresh, 15, 30, and 60 seconds. Default is No Refresh.
- **Frames Received** — Displays the number of valid EAPOL frames received on the port.
- **Frames Transmitted** — Displays the number of EAPOL frames transmitted through the port.
- **Start Frames Received** — Displays the number of EAPOL Start frames received on the port.
- **Log off Frames Received** — Displays the number of EAPOL Log off frames that have been received on the port.
- **Respond ID Frames Received** — Displays the number of EAP Respond ID frames that have been received on the port.

Downloaded from www.Manualslib.com manuals search engine

- **Respond Frames Received** — Displays the number of valid EAP Respond frames received on the port.
- **Request ID Frames Received** — Displays the number of EAP Request ID frames that have been received on the port.
- **Request Frames Transmitted** — Displays the number of EAP Request frames transmitted through the port.
- **Request ID Frames Transmitted** — Displays the number of EAP Requested ID frames transmitted through the port.
- **Invalid Frames Received** — Displays the number of unrecognized EAPOL frames received on this port.
- **Length Error Frames Received** — Displays the number of EAPOL frames with an invalid Packet Body Length received on this port.
- **Last Frames Version** — Displays the protocol version number attached to the most recently received EAPOL frame.
- **Last Frames Source** — Displays the source MAC Address attached to the most recently received EAPOL frame.

Displaying EAP statistics for an Interface

1. Open the **EAP Statistics** page.
2. Select an interface in the **Interface** field.

   The EAP statistics for the selected interface display.

Viewing EAP Statistics Using the CLI Command

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- 802.1X Commands

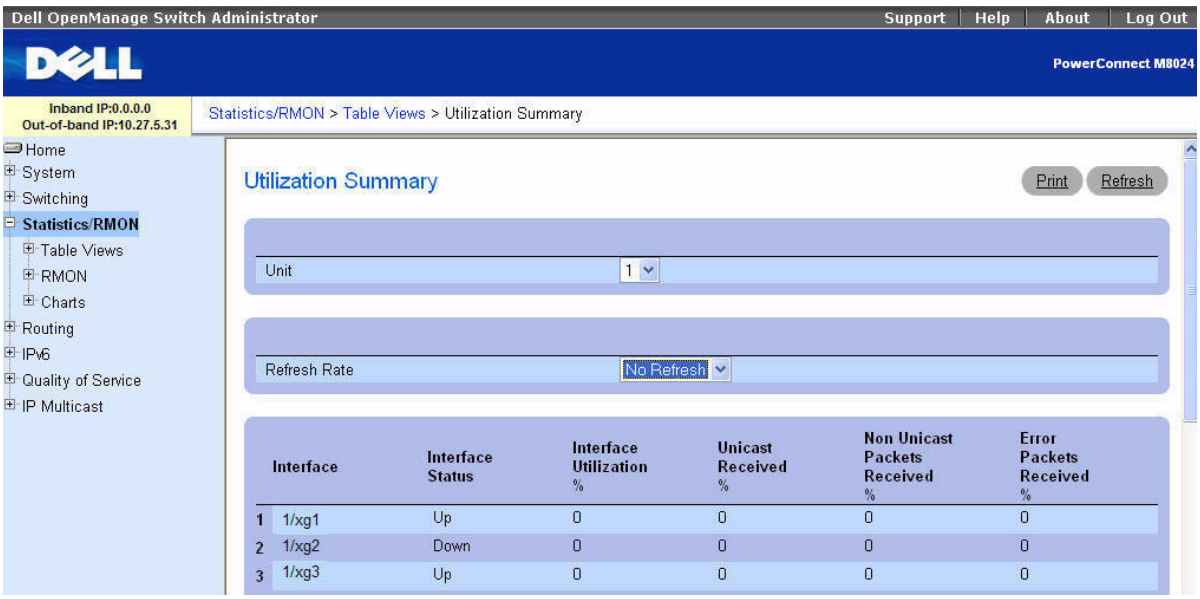
Downloaded from www.Manualslib.com manuals search engine

Utilization Summary

Use the **Utilization Summary** page to display interface utilization statistics.

To display the page, click **Statistics/RMON > Table Views > Utilization Summary** in the tree view.

Figure 8-5. Utilization Summary



The **Utilization Summary** page contains the following fields:

- **Unit** — Specifies the unit for which statistics are displayed.
- **Refresh Rate** — Specifies amount of time that passes before statistics are refreshed. The possible field values are No Refresh, 15, 30, and 60 seconds. Default is No Refresh.
- **Interface** — Specifies the interface for which statistics are displayed.
- **Interface Status** — Displays status of the interface.
- **Interface Utilization %** — Displays network interface utilization percentage based on the duplex mode of the interface. The range of this reading is from 0 to 200%. The maximum reading of 200% for a full duplex connection indicates that 100% of bandwidth of incoming and outgoing connections is used by the traffic travelling through the interface. The maximum reading for a half duplex connection is 100%.
- **Unicast Received %** — Displays percentage of Unicast packets received on the interface.
- **Non Unicast Packets Received %** — Displays percentage of non-Unicast packets received on the interface.
- **Error Packets Received %** — Displays number packets with errors received on the interface.

Downloaded from www.Manualslib.com manuals search engine

Viewing Interface Utilization Statistics Using the CLI Command

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

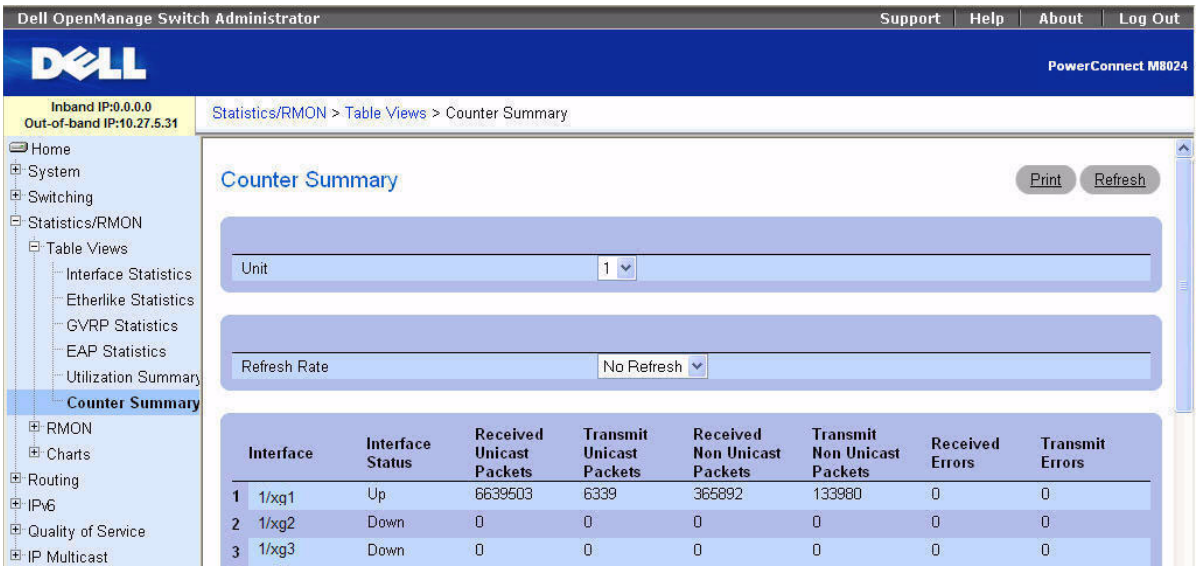
- RMON Commands

Counter Summary

Use the **Counter Summary** page to display interface utilization statistics in numeric sums as opposed to percentages.

To display the page, click **Statistics/RMON > Table Views > Counter Summary** in the tree view.

Figure 8-6. Counter Summary



The **Counter Summary** page contains the following fields:

- **Unit** — Specifies the unit for which statistics are displayed.
- **Refresh Rate** — Specifies amount of time that passes before statistics are refreshed. The possible field values are No Refresh, 15, 30, and 60 seconds. Default is No Refresh.
- **Interface** — Specifies the interface for which statistics are displayed.
- **Interface Status** — Displays status of the interface.
- **Received Unicast Packets** — Displays number of received Unicast packets on the interface.
- **Transmit Unicast Packets** — Displays number of transmitted Unicast packets from the interface.
- **Received Non Unicast Packets** — Displays number of received non-Unicast packets on the interface.
- **Transmit Non Unicast Packets** — Displays number of transmitted non-Unicast packets from the interface.

Downloaded from www.Manualslib.com manuals search engine

- **Received Errors**— Displays number of received errors on the interface.
- **Transmit Errors** — Displays number of transmitted errors from the interface.

Setting Refresh Rate

1. Open the **Counter Summary** page.
2. Select the **Refresh Rate** from the drop-down menu.

   Statistics refresh for the displayed interfaces at the selected frequency.

Viewing Numeric Port Utilization Statistics Using the CLI Command

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- RMON Commands

RMON

Remote monitoring (RMON) allows the network administrator to get an idea of the network's performance and status through remote access.

To display the **RMON** menu page, click **Statistics/RMON > RMON** in the tree view. The **RMON** menu page contains links to the following features:

- RMON Statistics
- RMON History Control Statistics
- RMON History Table
- RMON Event Control
- RMON Event Log
- RMON Alarms

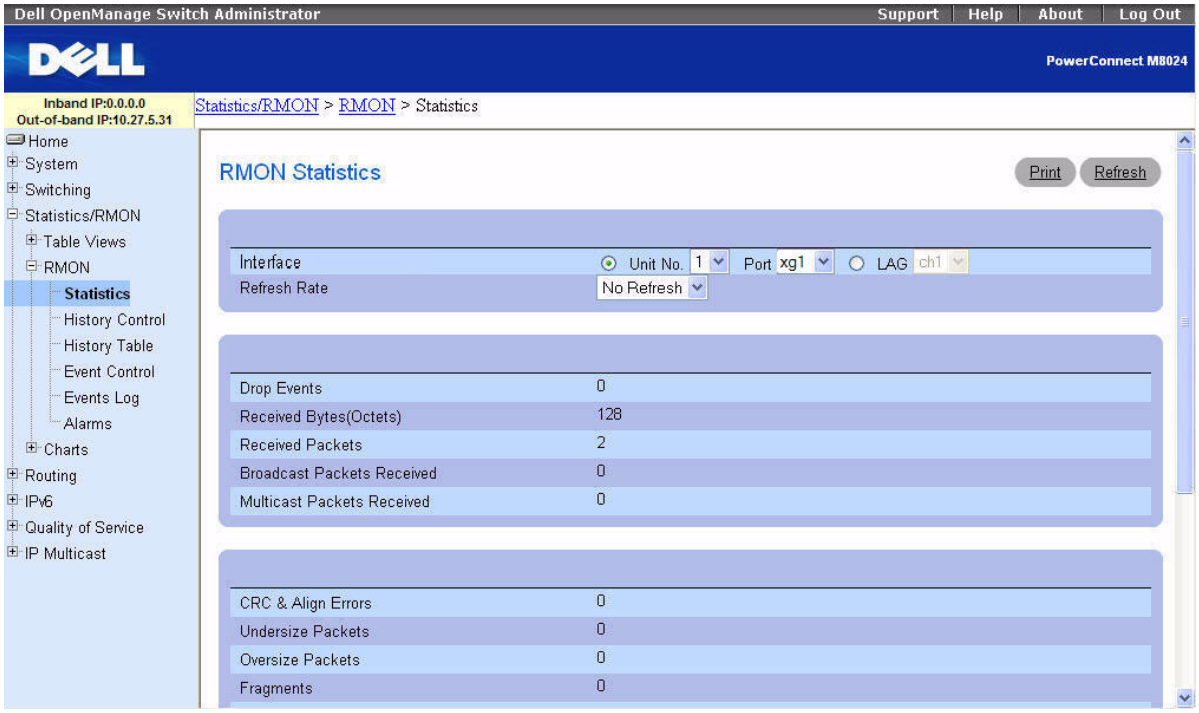
Downloaded from www.Manualslib.com manuals search engine

RMON Statistics

Use the **RMON Statistics** page to display details about switch use such as packet processing statistics and errors that have occurred on the switch.

To display the page, click **Statistics/RMON** > **RMON** > **Statistics** in the tree view.

Figure 8-7. RMON Statistics



The **RMON Statistics** page contains the following fields:

- **Interface** — Specifies whether statistics are shown for a Unit or a LAG as well as which Unit/LAG is displayed.
- **Refresh Rate** — Specifies amount of time that passes before statistics are refreshed. The possible field values are No Refresh, 15, 30, and 60 seconds. Default is No Refresh.
- **Drop Events** — Displays number of dropped events that have occurred on the interface since the switch was last refreshed.
- **Received Bytes (Octets)** — Displays number of octets received on the interface since the switch was last refreshed. This number includes bad packets and FCS octets, but excludes framing bits.
- **Received Packets** — Displays number of packets received on the interface, including bad packets, multicast and broadcast packets, since the switch was last refreshed.
- **Broadcast Packets Received** — Displays number of good broadcast packets received on the interface since the switch was last refreshed. This number does not include multicast packets.

Downloaded from www.Manualslib.com manuals search engine

- **Multicast Packets Received** — Displays number of good multicast packets received on the interface since the switch was last refreshed.
- **CRC & Align Errors** — Displays number of CRC and Align errors that have occurred on the interface since the switch was last refreshed.
- **Undersize Packets** — Displays number of undersized packets (less than 64 octets) received on the interface since the switch was last refreshed.
- **Oversize Packets** — Displays number of oversized packets (over 1518 octets) received on the interface since the switch was last refreshed.
- **Fragments** — Displays number of fragments (packets with less than 64 octets, excluding framing bits, but including FCS octets) received on the interface since the switch was last refreshed.
- **Jabbers** — Displays number of packets received that were more than 1,518 octets long and had a FCS during the sampling session.
- **Collisions** — Displays number of collisions received on the interface since the switch was last refreshed.
- **Frames of 64 Bytes** — Displays number of 64-byte frames received on the interface since the switch was last refreshed.
- **Frames of 65 to 127 Bytes** — Displays number of 65- to127-byte frames received on the interface since the switch was last refreshed.
- **Frames of 128 to 255 Bytes** — Displays number of 128- to 255-byte frames received on the interface since the switch was last refreshed.
- **Frames of 256 to 511 Bytes** — Displays number of 256- to 511-byte frames received on the interface since the switch was last refreshed.
- **Frames of 512 to 1023 Bytes** — Displays number of 512- to 1023-byte frames received on the interface since the switch was last refreshed.
- **Frames of 1024 to 1518 Bytes** — Displays number of 1024- to 1518-byte frames received on the interface since the switch was last refreshed.

Viewing Interface Statistics

1. Open the **RMON Statistics Group** page.
2. Select an interface in the **Interface** field.

   Statistics for the selected interface display.

Viewing RMON Statistics Using the CLI Command

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- RMON Commands

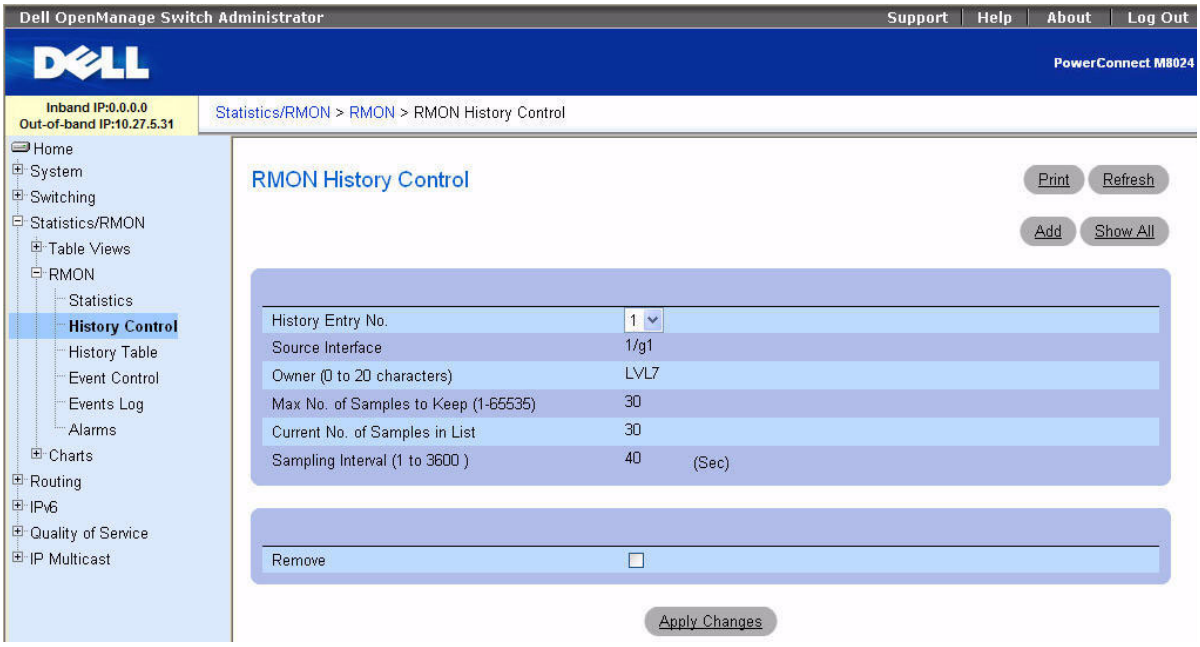
Downloaded from www.Manualslib.com manuals search engine

RMON History Control Statistics

Use the **RMON History Control** page to maintain a history of statistics on each port. For each interface (either a physical port or a port-channel), you can define how many buckets exist, and the time interval between each bucket snapshot.

To display the page, click **Statistics/RMON > RMON > History Control** in the tree view.

Figure 8-8. RMON History Control



The **RMON History Control** page contains the following fields:

- **History Entry** — Selects entry number on the **RMON History Control Table**.
- **Source Interface** — Specifies interface from which the history samples are taken.
- **Owner (0–20 characters)** — Indicates RMON station or user that requested the RMON information.
- **Max No. of Samples to Keep (1–65535)** — Sets the number of historical buckets for this interface.
- **Current No. of Samples in List** — Displays the current number of samples taken.
- **Sampling Interval (1–3600)** — Sets the frequency at which samplings are taken from the ports. The possible values are from 1 to 3600 seconds. The default is 1800 seconds (30 minutes).
- **Remove** — Removes the **RMON History Control Table** entry displayed when checked.

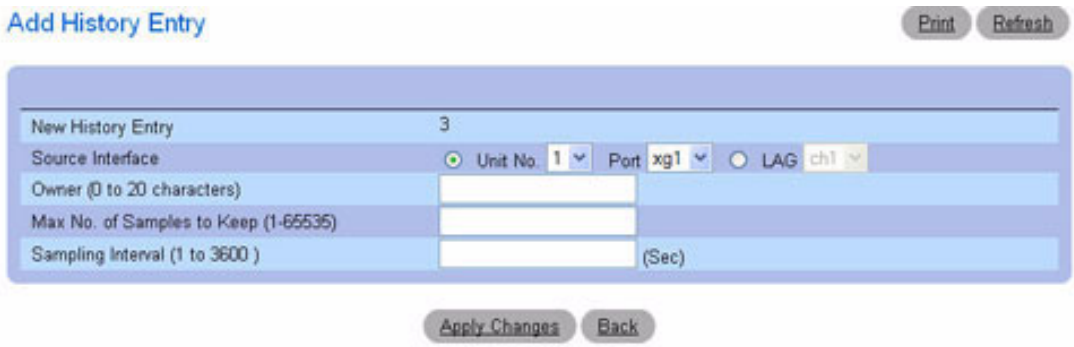
Downloaded from www.Manualslib.com manuals search engine

Adding a History Control Entry

1. Open the **RMON History Control** page.
2. Click **Add**.

   The **Add History Entry** page displays.

Figure 8-9. Add History Entry



3. Complete the fields on this page and click **Apply Changes**.

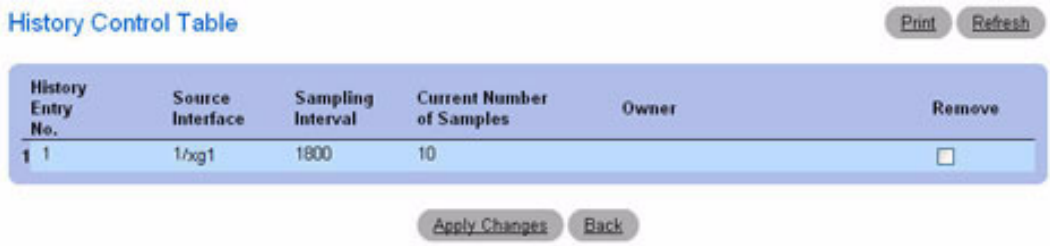
   The entry is added to the **RMON History Control Table**.

Displaying the RMON History Control Table

1. Open the **RMON History Control** page.
2. Click **Show All**.

   The **RMON History Control Table** displays.

Figure 8-10. RMON History Control Table



Removing a History Control Table Entry

1. Open the **RMON History Control** page.
2. Select the **Remove** check box in the row of the history entry to remove.
3. Click **Apply Changes**.

   The table entry is removed, and the device is updated.

Downloaded from www.Manualslib.com manuals search engine

Viewing RMON History Control Using the CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

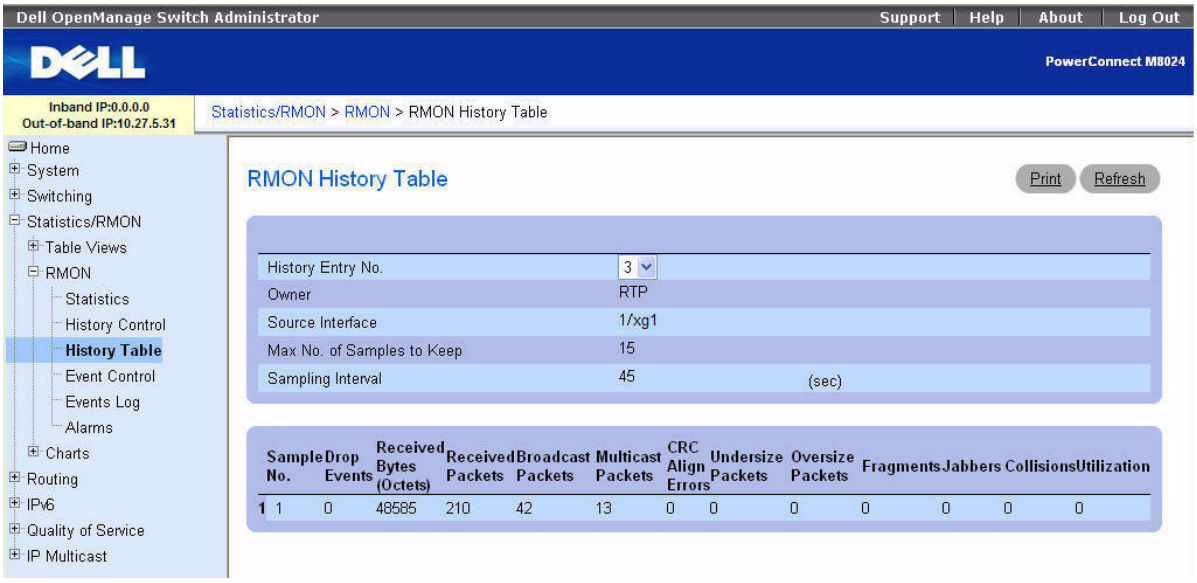
- RMON Commands

RMON History Table

Use the RMON History Table page to display interface-specific statistical network samplings. Each table entry represents all counter values compiled during a single sample.

To display the **RMON History Table** page, click **Statistics/RMON > RMON > History Table** in the tree view.

Figure 8-11. RMON History Table



The **RMON History Table** page contains the following fields:

- **History Entry No.** — Selects the history entry number to display on the RMON **History Table**.
- **Owner** — Displays RMON statistics group owner name, if available.
- **Source Interface** — Indicates the Interface or LAG where the statistics are being collected.
- **Max No. of Samples to Keep** — Determines the length of the list in the History table for each History Entry No.
- **Sampling Interval** — Sets the time in seconds between successive samples.
- **Sample No.** — Indicates the specific sample the information in the table reflects.

Downloaded from www.Manualslib.com manuals search engine

- **Drop Events** — Displays the total number of events in which packets were dropped by the port due to lack of resources. Note that this number is not necessarily the number of packets dropped; it is just the number of times this condition has been detected.
- **Received Bytes (Octets)**— Displays the total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including Frame Check Sequence (FCS) octets).
- **Received Packets** — Displays the total number of packets received (including bad packets, broadcast packets, and multicast packets) during the sampling interval.
- **Broadcast Packets** — Displays the total number of good packets received that were directed to the broadcast address. Note that this does not include multicast packets.
- **Multicast Packets** — Displays the total number of good packets received that were directed to a multicast address. Note that this number does not include packets directed to the broadcast address.
- **CRC Align Errors** — Displays the total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad FCS with an integral number of octets, (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
- **Undersize Packets** — Displays the total number of packets received that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well formed.
- **Oversize Packets** — Displays the total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.
- **Fragments** — Displays the total number of packets received that were less than 64 octets in length (excluding framing bits but including (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
- **Jabbers** — Displays the total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error), or a bad FCS with a non-integral number of octets (Alignment Error).
- **Collisions** — Displays the best estimate of the total number of collisions on this Ethernet segment.
- **Utilization** — Estimates the main physical layer network usage on an interface during the session sampling. The value is reflected hundredths of percent.

Viewing Statistics for a Specific History Entry

1. Open the **RMON History Table** page.
2. Select an entry in the **History Entry No.** field.

   The entry's statistics display on screen.

Downloaded from www.Manualslib.com manuals search engine

Viewing RMON History Control Using the CLI Command

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

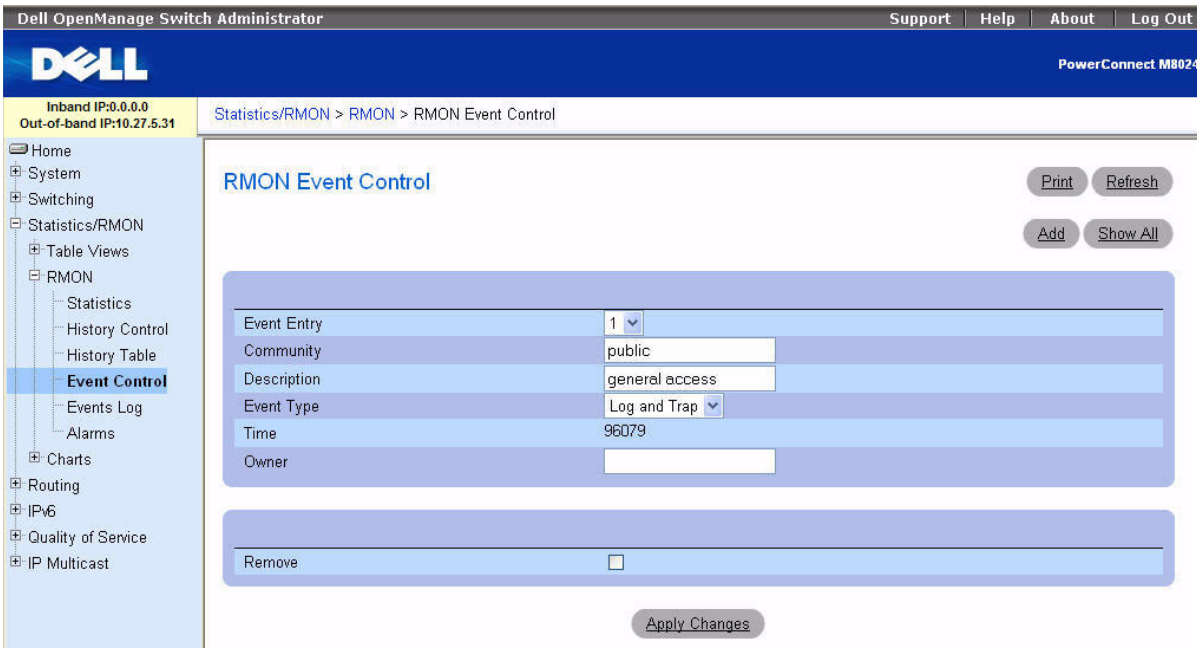
- RMON Commands

RMON Event Control

Use the **RMON Events Control** page to define RMON events. Events are used by RMON alarms to force some action when a threshold is crossed for a particular RMON counter. The event information can be stored in a log and/or sent as a trap to a trap receiver.

To display the page, click **Statistics/RMON > RMON > Event Control** in the tree view.

Figure 8-12. RMON Event Control



Downloaded from www.Manualslib.com manuals search engine

The **RMON Event Control** page contains the following fields:

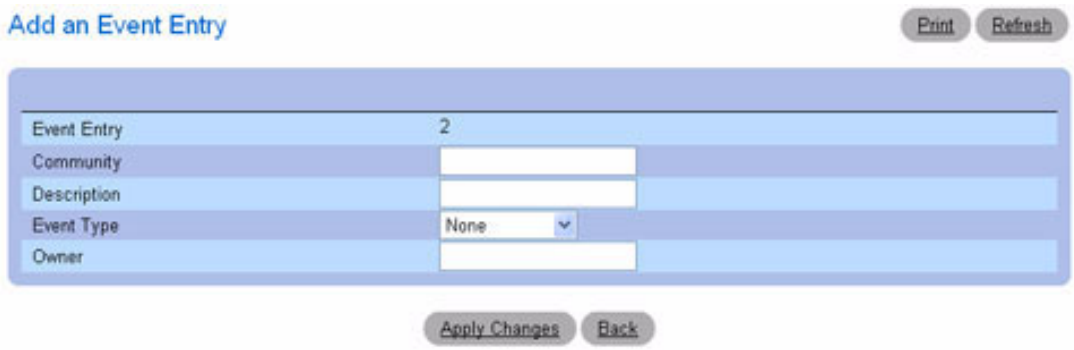
- **Event Entry** — Selects the event.
- **Community** — Specifies the community to which the event belongs.
- **Description** — Describes the user-defined event.
- **Event Type** — Selects the event type. Possible values are:
  - **Log** — Event type is a log entry.
  - **Trap** — Event type is a trap.
  - **Log and Trap** — Event type is both a log entry and a trap.
  - **None** — There is no event.
- **Time** — Displays the time when the event occurred.
- **Owner** — Lists the switch or user that defined the event.
- **Remove** — Removes the event from the Events Table when checked.

Adding an RMON Event

1. Open the **RMON Event Control** page.
2. Click **Add**.

   The **Add an Event Entry** page displays.

Figure 8-13. Add an Event Entry



3. Complete the fields on this page.
4. Click **Apply Changes**.

   The event is added to the **RMON Event Table**, and the device is updated.

Downloaded from www.Manualslib.com manuals search engine

Modifying an RMON Event

1. Open the **RMON Event Control** page.
2. Click **Show All** to display the **Event Control Table** page.
3. Select the **Edit** check box in for the event entry to change.
4. Modify the fields on the page as needed.
5. Click **Apply Changes**.

   The **RMON Events Table** entry is modified, and the device is updated.

Displaying the RMON Event Control Table

1. Open the **RMON Event Control** page.
2. Click **Show All**.

   The **Event Control Table** displays.

Figure 8-14. Event Control Table

Removing RMON Event Entries

1. Open the **RMON Event Control** page.
2. Choose the event to remove from the drop-down menu in the **Event Entry** field and check **Remove.**
3. Click **Apply Changes**.

   The table entry is removed, and the device is updated.

Defining Switch Events Using the CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- RMON Commands

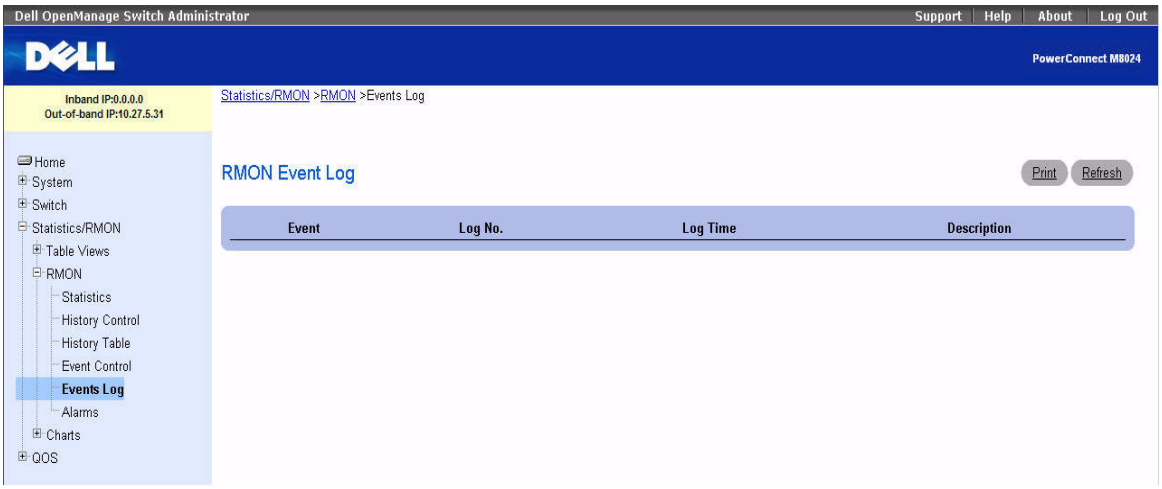
Downloaded from www.Manualslib.com manuals search engine

RMON Event Log

Use the **RMON Event Log** page to display a list of RMON events.

To display the page, click **Statistics/RMON > RMON > Events Log** in the tree view.

Figure 8-15. RMON Event Log



The **RMON Event Log** page contains the following fields:

- **Event** — Displays the RMON Events Log entry number.
- **Log No.** — Displays the log number.
- **Log Time** — Displays the time when the log entry was entered.
- **Description** — Describes the log entry.

Defining Switch Events Using the CLI Command

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- RMON Commands

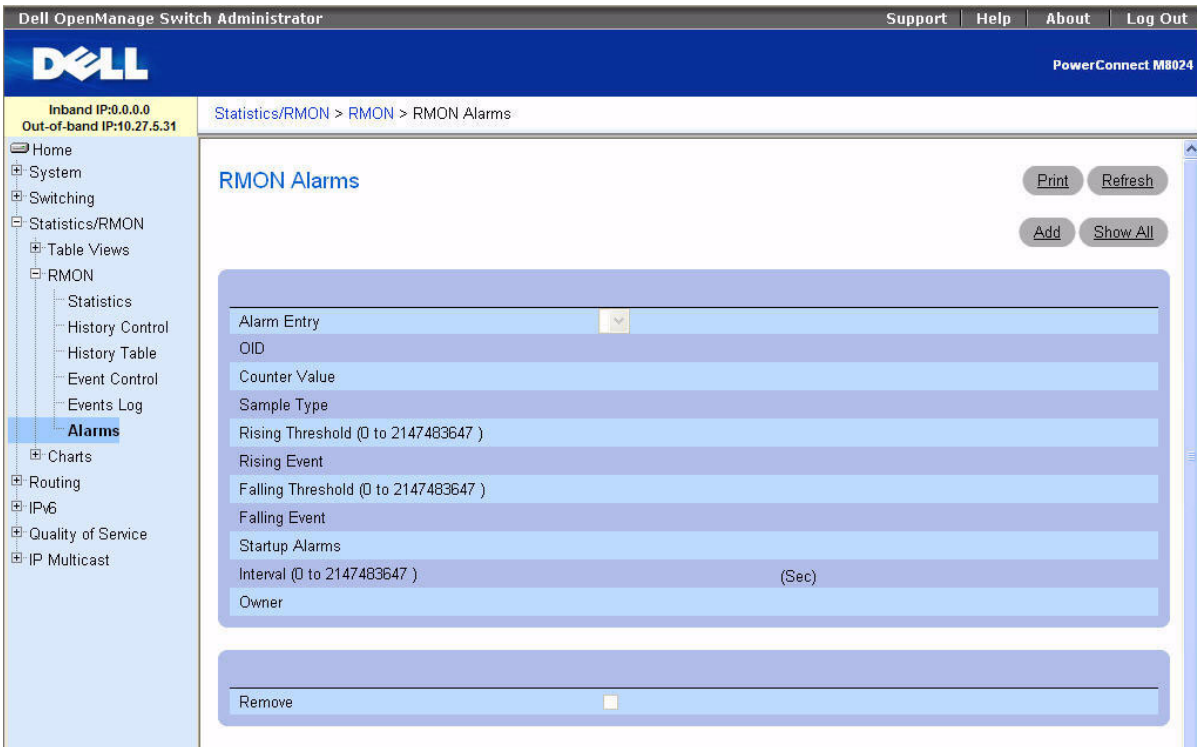
Downloaded from www.Manualslib.com manuals search engine

RMON Alarms

Use the **RMON Alarms** page to set network alarms. Alarms occur when certain thresholds are crossed for the configured RMON counters. The alarm triggers an event to occur. The events can be configured as part of the RMON Events group. For more information about events, see "RMON Event Log."

To display the page, click **Statistics/RMON > RMON > Alarms** in the tree view.

Figure 8-16. RMON Alarms



The **RMON Alarms** page contains the following fields:

- **Alarm Entry** — Selects a specific alarm from the drop-down menu.
- **OID** — Specifies the Object Identifier.
- **Counter Value —** Displays the number of selected events counted.
- **Sample Type** — Displays the sampling method for the selected variable and comparing the value against the thresholds. The possible field values are:
  - **Delta** — Subtracts the last sampled value from the current value. The difference in the values is compared to the threshold.
  - **Absolute** — Compares the values directly with the thresholds at the end of the sampling interval. This is the default.

Downloaded from www.Manualslib.com manuals search engine

- **Rising Threshold (0–2147483647)** — Displays the rising counter value that triggers the rising threshold alarm. The rising threshold is presented on top of the graph bars. Each monitored variable is designated a color. The default is 100.
- **Rising Event** — Displays the mechanism in which the alarms are reported, including a log, a trap, or both. When a log is selected, there is no saving mechanism either in the switch or in the management system. However, if the switch is not being reset, the event remains in the switch Log table. If a trap is selected, an SNMP trap is generated and reported through the Trap mechanism. The trap can be saved using the same mechanism.
- **Falling Threshold (0–2147483647)** — Displays the falling counter value that triggers the falling threshold alarm. The falling threshold is graphically presented on top of the graph bars. Each monitored variable is designated a color. The default is 20.
- **Falling Event** — Displays the mechanism in which the alarms are reported, including a log, a trap, or both. When a log is selected, there is no saving mechanism either in the switch or in the management system. However, if the switch is not being reset, the event remains in the switch Log table. If a trap is selected, an SNMP trap is generated and reported through the Trap mechanism. The trap can be saved using the same mechanism.
- **Startup Alarms** — Displays the type of event. Options are rising, rising-falling, and falling.
- **Interval (0–2147483647)**— Displays alarm interval time. The default is 100.
- **Owner** — Displays switch or user that defined the alarm.
- **Remove** — Removes an RMON Alarm when checked.

Adding an Alarm Table Entry

1. Open the **RMON Alarms** page.
2. Click **Add.**

   The **Add an Alarm Entry** page displays.

Downloaded from www.Manualslib.com manuals search engine

Figure 8-17. Add an Alarm Entry

3. Complete the fields on this page as needed.
4. Click **Apply Changes**.

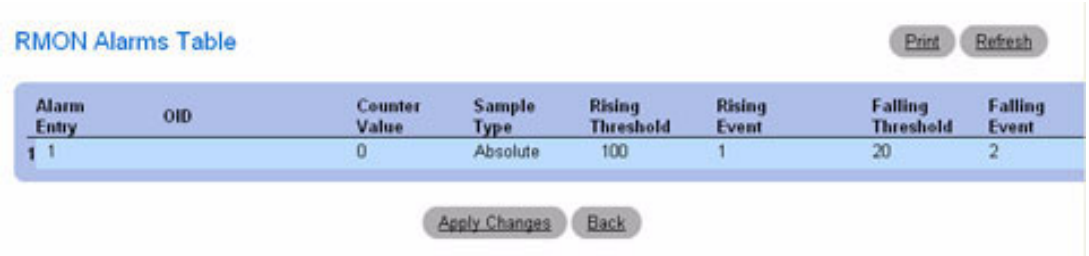
   The RMON alarm is added, and the device is updated.

Displaying the Alarm Table

1. Open the **RMON Alarms** page.
2. Click **Show All.**

   The left side of the **RMON Alarms Table** displays.

Figure 8-18. RMON Alarms Table



3. Click the right arrow at the bottom of the screen to view the right side of the table.

Downloaded from www.Manualslib.com manuals search engine

Removing One Alarm Table Entry

1. Open the **RMON Alarms** page.
2. Select an entry in the **Alarm Entry** drop-down menu.
3. Check the **Remove** check box and click **Apply Changes**.

   The entry is removed, and the device is updated.

Removing Multiple Alarm Table Entries

1. Open the **RMON Alarms** page.
2. Click **Show All.**

   The **RMON Alarms Table** displays.
3. Check **Remove** for each Alarm Entry to remove.
4. Click **Apply Changes**.

   The entries are removed, and the device is updated.

Defining Switch Alarms Using the CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- RMON Commands

Downloaded from www.Manualslib.com manuals search engine

Charts

The **Chart** menu page contains links to web pages that allow you to chart statistics on a graph. To display the **Charts** menu page, click **Statistics/RMON** > **Charts** in the tree view. The **Charts** menu page contains links to the following features:

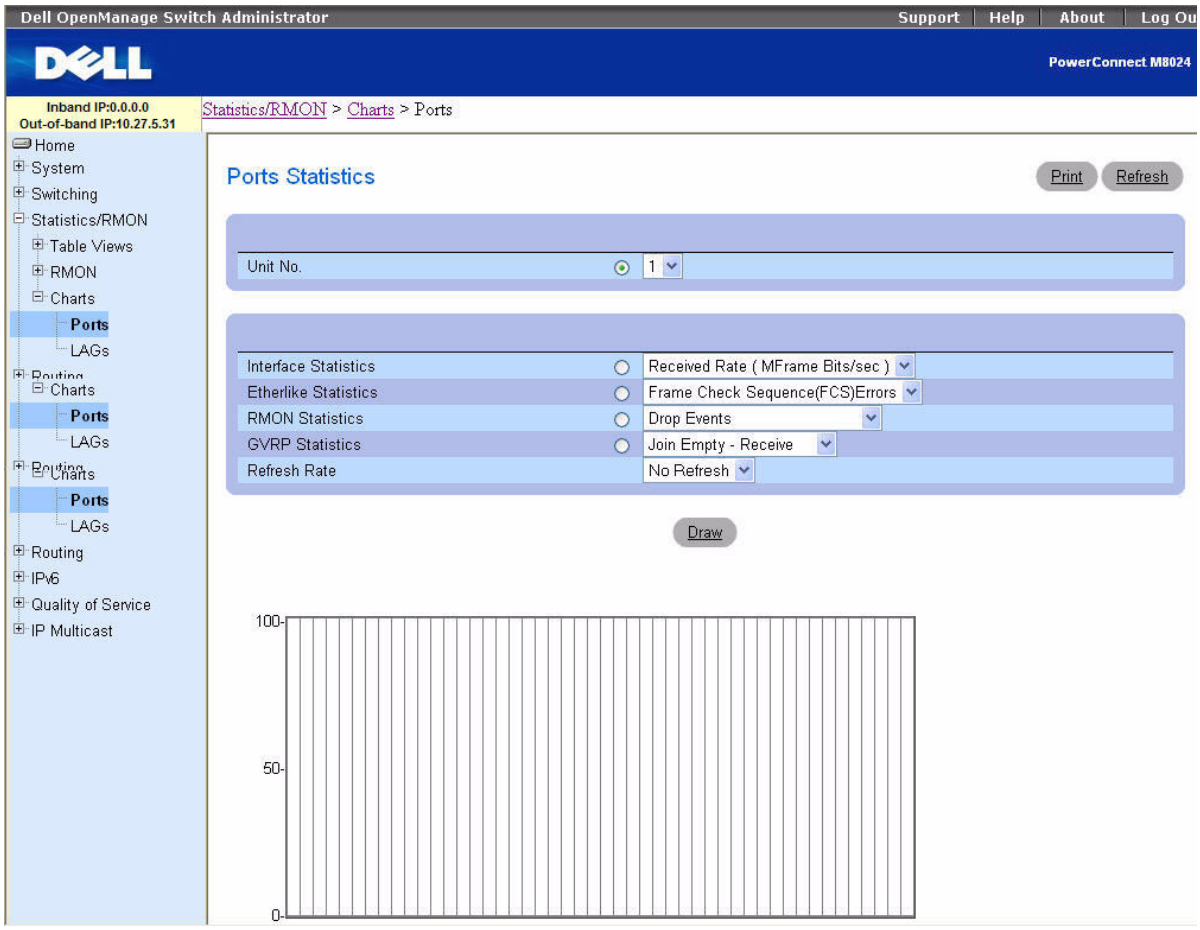
- Ports Statistics
- LAG Statistics

Ports Statistics

Use the **Ports Statistics** page to chart port-related statistics on a graph.

To display the page, click **Statistics/RMON** > **Charts** > **Ports** in the tree view.

Figure 8-19. Ports Statistics



Downloaded from www.Manualslib.com manuals search engine

The **Ports Statistics** page contains the following fields:

- **Unit No.** — Selects the port to be displayed.
- **Interface Statistics** — Selects Interface Statistics when clicked, and specifies the type of interface statistics to graph from the drop-down menu. The default is Received Rate (MFrame Bits/sec).
- **Etherlike Statistics** — Selects Etherlike Statistics when clicked, and specifies the type of etherlike statistics to graph from the drop-down menu. The default is Frame Check Sequence (FCS) Errors.
- **RMON Statistics** — Selects RMON Statistics when clicked, and specifies the type of RMON statistics to graph from the drop-down menu. The default is Drop Events.
- **GVRP Statistics** — Selects GVRP Statistics when clicked, and specifies the type of GVRP statistics to graph from the drop-down menu. The default is Join Empty - Receive.
- **Refresh Rate** — Selects the amount of time that passes before statistics are refreshed. The possible field values are No Refresh, 15, 30 and 60 seconds. The default rate is No Refresh.

Displaying Port Statistics

1. Open the **Ports Statistics** page.
2. Select the port for which statistics will be charted.
3. Click the radio button associated with the statistics to chart.
4. Select the type of statistics from the related drop-down menu.
5. Select the desired refresh rate from the **Refresh Rate** drop-down menu.
6. Click **Draw**.

   The selected statistics are charted on the graph.

Viewing Port Statistics Using the CLI Commands

For information about the CLI commands that perform this function, see the following chapters in the *CLI Reference Guide*:

- System Management Commands
- RMON Commands
- GVRP Commands

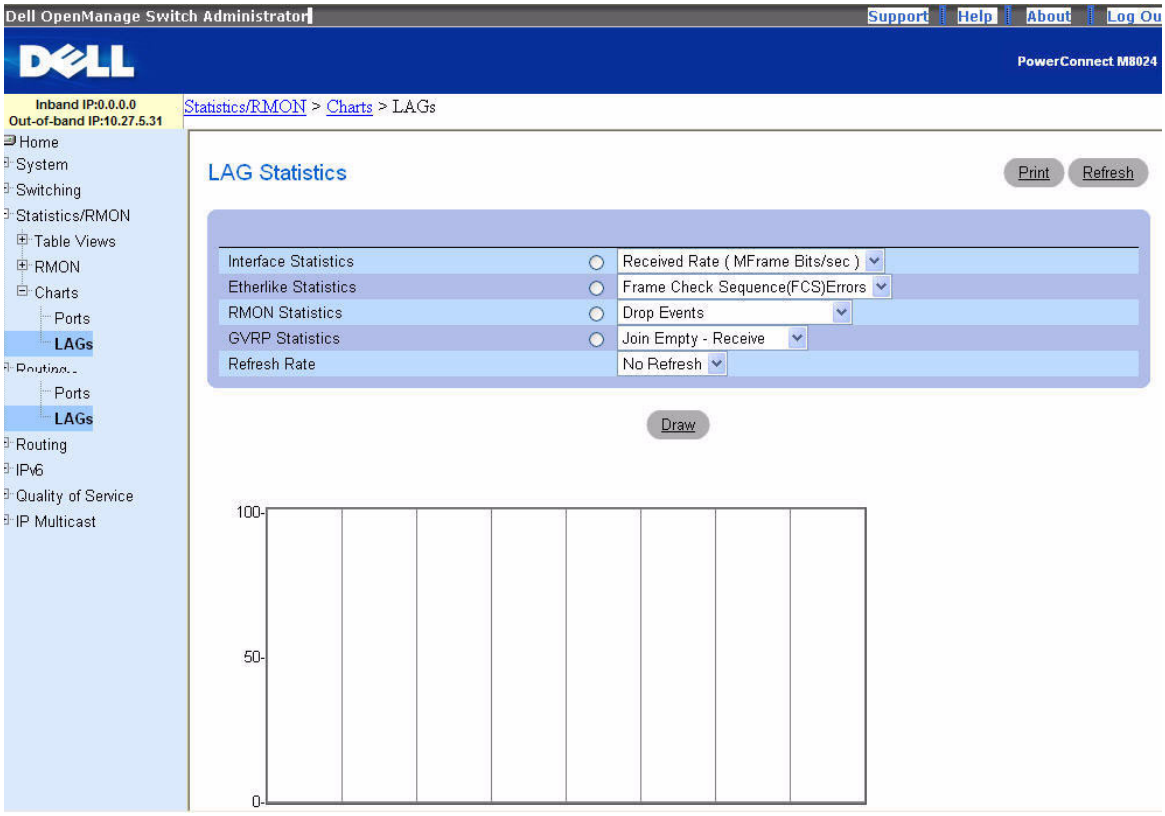
Downloaded from www.Manualslib.com manuals search engine

LAG Statistics

Use the **LAG Statistics** page to chart LAG-related statistics on a graph.

To display the page, click **Statistics/RMON > Charts > LAGs** in the tree view.

Figure 8-20. LAG Statistics



The **LAG Statistics** page contains the following fields:

- **Interface Statistics** — Selects Interface Statistics when clicked, and specifies the type of interface statistics to graph from the drop-down menu. The default is Received Rate.
- **Etherlike Statistics** — Selects Etherlike Statistics when clicked, and specifies the type of etherlike statistics to graph from the drop-down menu. The default is Frame Check Sequence Errors.
- **RMON Statistics** — Selects RMON Statistics when clicked, and specifies the type of RMON statistics to graph from the drop-down menu. The default is Drop Events.
- **GVRP Statistics** — Selects GVRP Statistics when clicked, and specifies the type of GVRP statistics to graph from the drop-down menu. The default is Join Empty - Receive.
- **Refresh Rate** — Selects the amount of time that passes before statistics are refreshed. The possible field values are No Refresh, 15, 30 and 60 seconds. The default rate is 15 seconds.

Downloaded from www.Manualslib.com manuals search engine

Displaying LAG Statistics

1. Open the **LAG Statistics** page.
2. Click the radio button associated with the statistics to chart.
3. Select the type of statistics from the related drop-down menu.
4. Select the desired refresh rate from the **Refresh Rate** drop-down menu.
5. Click **Draw**.

   The selected statistics are charted on the graph.

Viewing LAG Statistics Using the CLI Commands

For information about the CLI commands that perform this function, see the following chapters in the *CLI Reference Guide*:

- System Management Commands
- RMON Commands
- GVRP Commands

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

9

Configuring Routing

Overview

The PowerConnect M6220/M6348/M8024 supports the IP routing feature. Use the **Routing** menu page to configure routing on VLANs.

When a packet enters the switch, the destination MAC address is checked to see if it matches any of the configured routing interfaces. If it does, then the device searches the host table for a matching destination IP address. If an entry is found, then the packet is routed to the host. If there is not a matching entry, then the switch performs a longest prefix match on the destination IP address. If an entry is found, then the packet is routed to the next hop. If there is no match, then the packet is routed to the next hop specified in the default route. If there is no default route configured, then the packet is passed to the PowerConnect M6220/M6348/M8024 software to be handled appropriately.

The routing table can have entries added either statically by the administrator or dynamically through RIP or OSPF. The host table can have entries added either statically by the administrator or dynamically through ARP.

The **Routing** menu page contains links to the following features:

- ARP
- IP
- OSPF
- BOOTP/DHCP Relay Agent
- IP Helper
- RIP
- Router Discovery
- Router
- VLAN Routing
- VRRP
- Tunnels
- Loopbacks

Note: CLI commands are not available for all the Routing pages.

Downloaded from www.Manualslib.com manuals search engine

ARP

The PowerConnect M6220/M6348/M8024 uses the ARP protocol to associate a layer 2 MAC address with a layer 3 IPv4 address. Additionally, the administrator can statically add entries into the ARP table.

ARP is a necessary part of the internet protocol (IP) and is used to translate an IP address to a media (MAC) address, defined by a local area network (LAN) such as Ethernet. A station needing to send an IP packet must learn the MAC address of the IP destination, or of the next hop router, if the destination is not on the same subnet. This is achieved by broadcasting an ARP request packet, to which the intended recipient responds by unicasting an ARP reply containing its MAC address. Once learned, the MAC address is used in the destination address field of the layer 2 header prepended to the IP packet.

The ARP cache is a table maintained locally in each station on a network. There are no specific requirements for the construction or maintenance of this cache, but at a minimum it needs to contain the information learned from processing ARP protocol packets, which for Ethernet are denoted by an 0x0806 EtherType field. ARP cache entries are learned by examining the source information in the ARP packet payload fields, regardless of whether it is an ARP request or response. Thus, when an ARP request is broadcast to all stations on a LAN segment or virtual LAN (VLAN), every recipient has the opportunity to store the sender's IP and MAC address in their respective ARP cache. The ARP response, being unicast, is normally seen only by the requestor, who stores the sender information in its ARP cache. Newer information always replaces existing content in the ARP cache.

The ARP cache can support 896 entries, although this size is user-configurable to any value between 256 and 896. When multiple network interfaces are supported by a device, as is typical of a router, either a single ARP cache is used for all interfaces, or a separate cache is maintained per interface. While the latter approach is useful when network addressing is not unique per interface, this is not the case for Ethernet MAC address assignment so a single ARP cache is employed.

Devices can be moved in a network, which means the IP address that was at one time associated with a certain MAC address is now found using a different MAC, or may have disappeared from the network altogether (i.e., it has been reconfigured, disconnected, or powered off). This leads to stale information in the ARP cache unless entries are updated in reaction to new information seen on the network, periodically refreshed to determine if an address still exists, or removed from the cache if the entry has not been identified as a sender of an ARP packet during the course of an ageout interval, usually specified through configuration.

The **ARP** menu page contains links to web pages that configure and display ARP detail. To display this page, click **Routing > ARP** in the tree view. Following are the web pages accessible from this menu page:

- ARP Create
- ARP Table Configuration

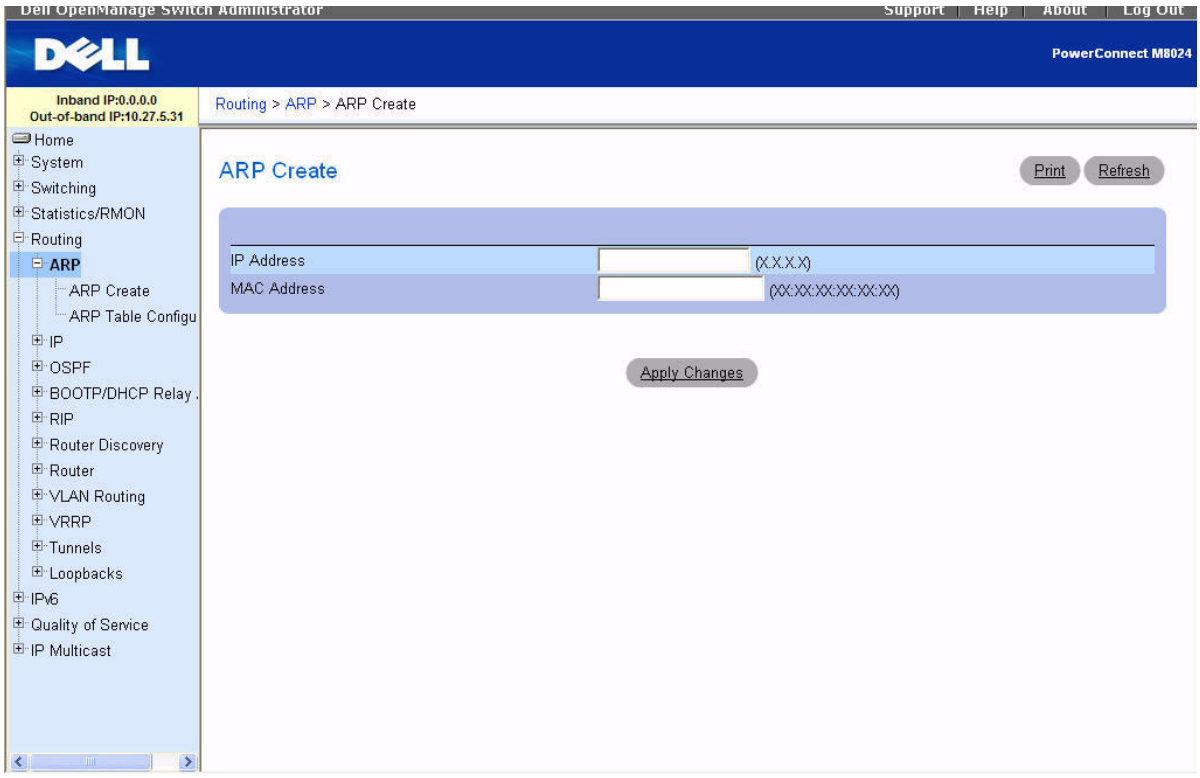
Downloaded from www.Manualslib.com manuals search engine

ARP Create

Use the **ARP Create** page to add an entry to the Address Resolution Protocol table.

To display the page, click **Routing > ARP > ARP Create** in the tree view.

Figure 9-1. ARP Create



The **ARP Create** page contains the following fields:

- **IP Address** — Enter the IP address you want to add. It must be the IP address of a device on a subnet attached to one of the switch's existing routing interfaces.
- **MAC Address** — The unicast MAC address of the device. Enter the address as six two-digit hexadecimal numbers separated by colons, for example 00:06:29:32:81:40.

Adding an Entry to the ARP Table

1. Open the **ARP Create** page.
2. Specify the addresses to be associated.
3. Click **Apply Changes**.

   The addresses are now in the ARP cache.

Downloaded from www.Manualslib.com manuals search engine

Adding Entries to the ARP Table using the CLI Command

For information about the CLI command that performs this function, see the following chapter in the *CLI Reference Guide*:

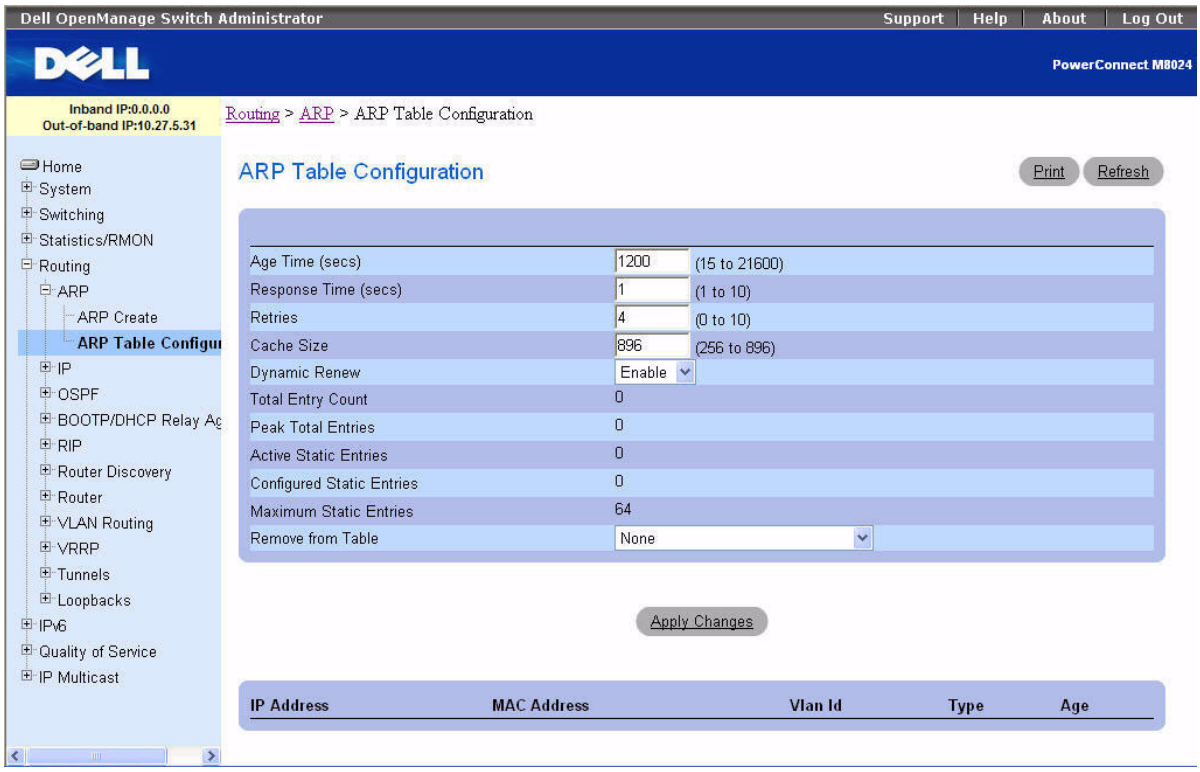
- ARP Commands

ARP Table Configuration

Use this page to change the configuration parameters for the Address Resolution Protocol Table. You can also use this screen to display the contents of the table.

To display the page, click **Routing > ARP > ARP Table Configuration** in the tree view.

Figure 9-2. ARP Table Configuration



Downloaded from www.Manualslib.com manuals search engine

The **ARP Table Configuration** page contains the following fields:

- **Age Time (secs)** — Enter the value you want the switch to use for the ARP entry ageout time. You must enter a valid integer, which represents the number of seconds it takes for an ARP entry to age out. The range for this field is 15 to 21600 seconds. The default value for Age Time is 1200 seconds.
- **Response Time** (secs) — Enter the value you want the switch to use for the ARP response timeout. You must enter a valid integer, which represents the number of seconds the switch waits for a response to an ARP request. The range for this field is 1 to 10 seconds. The default value for Response Time is 1 second.
- **Retries** — Enter an integer which specifies the maximum number of times an ARP request is retried. The range for this field is 0 to 10. The default value for Retries is 4.
- **Cache Size** — Enter an integer which specifies the maximum number of entries for the ARP cache. The range for this field is 256 to 896. The default value for Cache Size is 896.
- **Dynamic Renew** — This controls whether the ARP component automatically attempts to renew ARP Entries of type Dynamic when they age out. The default setting is Enable.
- **Total Entry Count** — Total number of Entries in the ARP table.
- **Peak Total Entries** — Highest value reached by Total Entry Count. This counter value is restarted whenever the ARP table Cache Size value is changed.
- **Active Static Entries** — Total number of Active Static Entries in the ARP table.
- **Configured Static Entries** — Total number of Configured Static Entries in the ARP table.
- **Maximum Static Entries** — Maximum number of Static Entries that can be defined.
- **Remove from Table** — Allows you to remove certain entries from the ARP Table. The choices listed specify the type of ARP Entry to be deleted:
  - All Dynamic Entries
  - All Dynamic and Gateway Entries
  - Specific Dynamic Gateway Entry
  - Specific Static Entry

The ARP Table displays at the bottom of the page, and contains the following fields:

- **IP Address** — The IP address of a device on a subnet attached to one of the switch's routing interfaces.
- **MAC Address** — The unicast MAC address for the device. The format is six two-digit hexadecimal numbers separated by colons, for example 00:06:29:32:81:40.
- **VLAN ID** — The routing interface associated with the ARP entry.
- **Type** — The type of the ARP entry.
- **Age** — Age since the entry was last refreshed in the ARP Table. The format is hh:mm:ss.

Downloaded from www.Manualslib.com manuals search engine

Configuring ARP Table

1. Open the **ARP Table Configuration** page.
2. Change parameters as needed.
3. Click **Apply Changes**.

   Changes are saved, and the ARP table is updated.

Configuring ARP Table with CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- ARP Commands

IP

The **IP** menu page contains links to web pages that configure and display IP routing data. To display this page, click **Routing > IP** in the tree view. Following are the web pages accessible from this menu page:

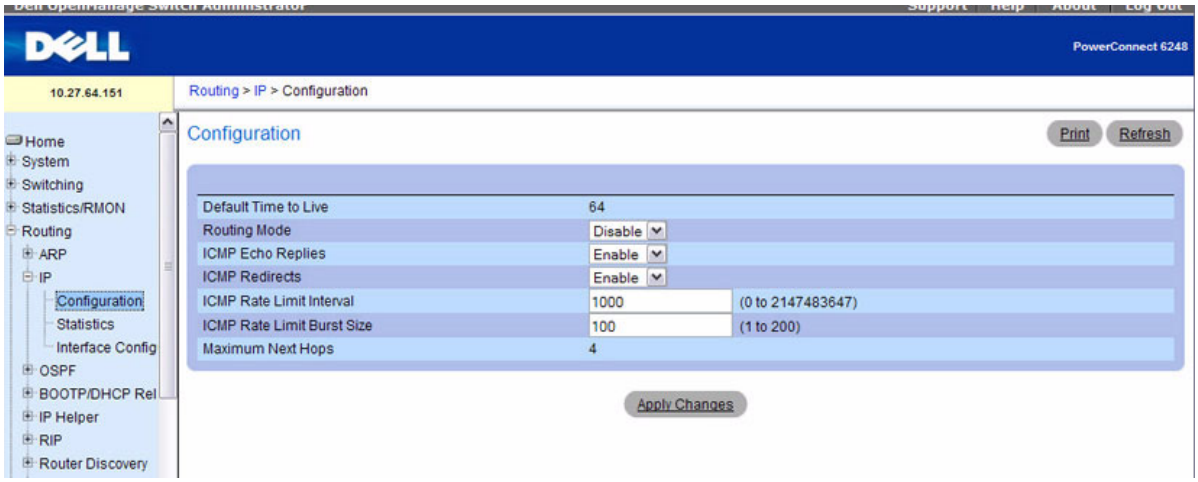
- IP Configuration
- IP Statistics
- IP Interface Configuration

IP Configuration

Use the IP **Configuration** page to configure routing parameters for the switch as opposed to an interface. The IP configuration settings allow you to enable or disable the generation of various types of ICMP messages.

To display the page, click **Routing > IP > Configuration** in the tree view.

Figure 9-3. IP Configuration



Downloaded from www.Manualslib.com manuals search engine

The **IP Configuration** page contains the following fields:

- **Default Time to Live** — The default value inserted into the Time-To-Live field of the IP header of datagrams originated by the switch, if a TTL value is not supplied by the transport layer protocol.
- **Routing Mode** — Select Enable or Disable from the drop-down menu. You must enable routing for the switch before you can route through any of the interfaces. Routing is also enabled or disabled per VLAN interface. The default value is Disable.
- **ICMP Echo Replies** —Select Enable to allow the switch to generate ECHO reply messages. Select Disable to prevent the switch from generating ICMP echo replies.
- **ICMP Redirects** — Select Enable to allow the switch to generate ICMP redirect messages. Select Disable to prevent the switch from generating ICMP redirect messages. The ICMP Redirect feature is also configurable on each interface.
- **ICMP Rate Limit Interval** — To control the ICMP error packets, you can specify the number of ICMP error packets that are allowed per burst interval. By default, the rate limit is 100 packets per second, i.e. the burst interval is 1000 milliseconds. To disable ICMP rate limiting, set this field to zero. The valid rate interval range is 0 to 2147483647 milliseconds.
- **ICMP Rate Limit Burst Size** — To control the ICMP error packets, you can specify the number of ICMP error packets that are allowed per burst interval. By default, the rate limit is 100 packets.
- **Maximum Next Hops** — The maximum number of hops supported by the switch. This is a compile-time constant.

Configuring IP Routing Parameters

1. Open the **IP Configuration** page.
2. Change parameters as needed.
3. Click **Apply Changes**.

   Changes are saved, and routing parameters are updated.

Configuring IP Routing Parameters with CLI Command

For information about the CLI commands that perform this function, see the following chapters in the *CLI Reference Guide:*

- IP Routing Commands
- VLAN Commands

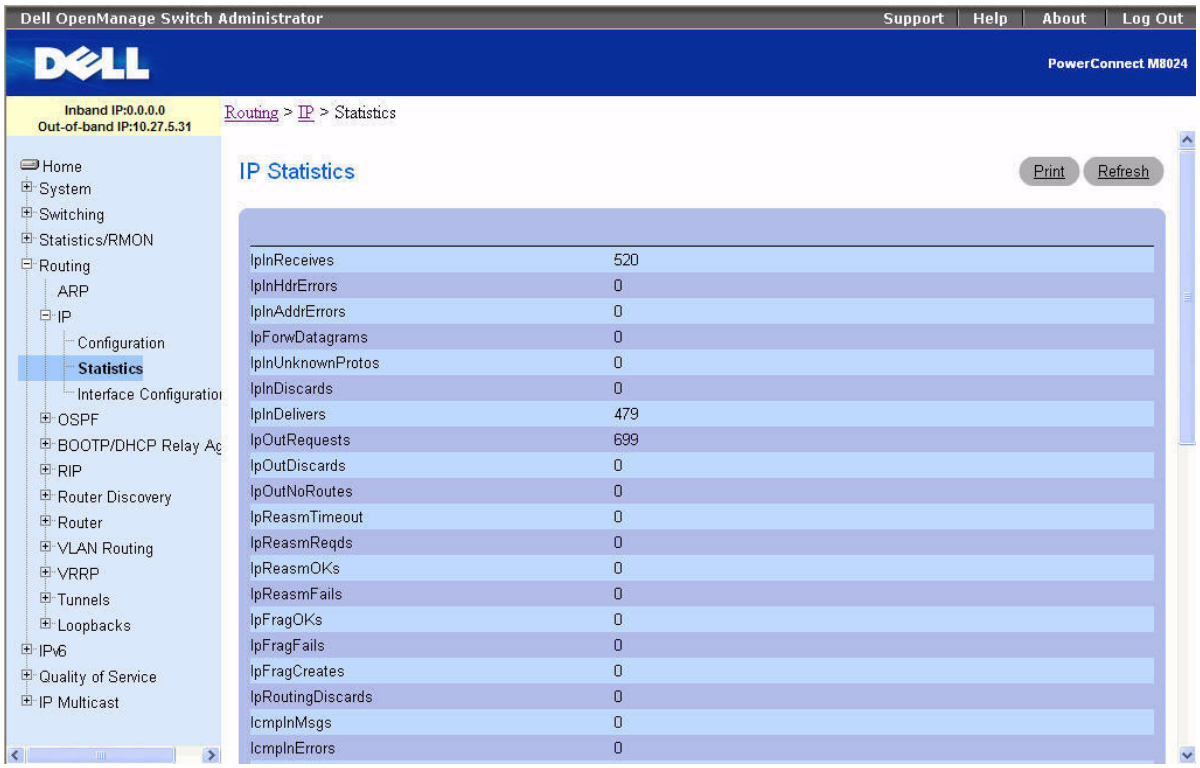
Downloaded from www.Manualslib.com manuals search engine

IP Statistics

The statistics reported on the **IP Statistics** page are as specified in RFC 1213.

To display the page, click **Routing > IP > Statistics** in the tree view.

Figure 9-4. IP Statistics



The **IP Statistics** page contains the following fields:

- **IpInReceives** — The total number of input datagrams received from interfaces, including those received in error.
- **IpInHdrErrors** — The number of input datagrams discarded due to errors in their IP headers, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, etc.
- **IpInAddrErrors** — The number of input datagrams discarded because the IP address in their IP header's destination field was not a valid address to be received at this entity. This count includes invalid addresses (for example, 0.0.0.0) and addresses of unsupported Classes (for example, Class E). For entities which are not IP Gateways and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.

Downloaded from www.Manualslib.com manuals search engine

- **IpForwDatagrams** — The number of input datagrams for which this entity was not their final IP destination, as a result of which an attempt was made to find a route to forward them to that final destination. In entities which do not act as IP Gateways, this counter includes only those packets which were Source-Routed through this entity, and the Source-Route option processing was successful.
- **IpInUnknownProtos** — The number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.
- **IpInDiscards** — The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (for example, for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting re-assembly.
- **IpInDelivers** — The total number of input datagrams successfully delivered to IP user-protocols (including ICMP).
- **IpOutRequests** — The total number of IP datagrams which local IP user-protocols (including ICMP) supplied to IP in requests for transmission. Note that this counter does not include any datagrams counted in ipForwDatagrams.
- **IpOutDiscards** — The number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (for example, for lack of buffer space). Note that this counter would include datagrams counted in ipForwDatagrams if any such packets met this (discretionary) discard criterion.
- **IpOutNoRoutes** — The number of IP datagrams discarded because no route could be found to transmit them to their destination. Note that this counter includes any packets counted in ipForwDatagrams which meet this `no-route' criterion and any datagrams which a host cannot route because all of its default gateways are down.
- **IpReasmTimeout** — The maximum number of seconds which received fragments are held while they are awaiting reassembly at this entity.
- **IpReasmReqds** — The number of IP fragments received which needed to be reassembled at this entity.
- **IpReasmOKs** — The number of IP datagrams successfully re-assembled.
- **IpReasmFails** — The number of failures detected by the IP re-assembly algorithm (for whatever reason: timed out, errors, and so on). Note that this is not necessarily a count of discarded IP fragments since some algorithms can lose track of the number of fragments by combining them as they are received.
- **IpFragOKs** — The number of IP datagrams that have been successfully fragmented at this entity.
- **IpFragFails** — The number of IP datagrams that have been discarded because they needed to be fragmented at this entity but could not be, for example, because their Don't Fragment flag was set.
- **IpFragCreates** — The number of IP datagram fragments that have been generated as a result of fragmentation at this entity.
- **IpRoutingDiscards** — The number of routing entries which were chosen to be discarded even though they are valid. One possible reason for discarding such an entry could be to free-up buffer space for other routing entries.

Downloaded from www.Manualslib.com manuals search engine

- **IcmpInMsgs** — The total number of ICMP messages which the entity received. Note that this counter includes all those counted by icmpInErrors.
- **IcmpInErrors** — The number of ICMP messages which the entity received but determined as having ICMP-specific errors (bad ICMP checksums, bad length, etc.).
- **IcmpInDestUnreachs** — The number of ICMP Destination Unreachable messages received.
- **IcmpInTimeExcds** — The number of ICMP Time Exceeded messages received.
- **IcmpInParmProbs** — The number of ICMP Parameter Problem messages received.
- **IcmpInSrcQuenchs** — The number of ICMP Source Quench messages received.
- **IcmpInRedirects** — The number of ICMP Redirect messages received.
- **IcmpInEchos** — The number of ICMP Echo (request) messages received.
- **IcmpInEchoReps** — The number of ICMP Echo Reply messages received.
- **IcmpInTimestamps** — The number of ICMP Timestamp (request) messages received.
- **IcmpInTimestampReps** — The number of ICMP Timestamp Reply messages received.
- **IcmpInAddrMasks** — The number of ICMP Address Mask Request messages received.
- **IcmpInAddrMaskReps** — The number of ICMP Address Mask Reply messages received.
- **IcmpOutMsgs** — The total number of ICMP messages which this entity attempted to send. Note that this counter includes all those counted by icmpOutErrors.
- **IcmpOutErrors** — The number of ICMP messages which this entity did not send due to problems discovered within ICMP such as a lack of buffers. This value should not include errors discovered outside the ICMP layer such as the inability of IP to route the resultant datagram. In some implementations there may be no types of error which contribute to this counter's value.
- **IcmpOutDestUnreachs** — The number of ICMP Destination Unreachable messages sent.
- **IcmpOutTimeExcds** — The number of ICMP Time Exceeded messages sent.
- **IcmpOutParmProbs** — The number of ICMP Parameter Problem messages sent.
- **IcmpOutSrcQuenchs** — The number of ICMP Source Quench messages sent.
- **IcmpOutRedirects** — The number of ICMP Redirect messages sent. For a host, this object is always zero, since hosts do not send redirects.
- **IcmpOutEchos** — The number of ICMP Echo (request) messages sent.
- **IcmpOutEchoReps** — The number of ICMP Echo Reply messages sent.
- **IcmpOutTimestamps** — The number of ICMP Timestamp (request) messages.
- **IcmpOutTimestampReps** — The number of ICMP Timestamp Reply messages sent.
- **IcmpOutAddrMasks** — The number of ICMP Address Mask Request messages sent.
- **IcmpOutAddrMaskReps** — The number of ICMP Address Mask Reply messages sent.

Downloaded from www.Manualslib.com manuals search engine

Refreshing IP Statistics

1. Open the **IP Statistics** page.
2. Click **Refresh**.

   The screen displays with the present state of the data in the switch.

Displaying IP Statistics using the CLI Command

For information about the CLI command that performs this function, see the following chapter in the *CLI Reference Guide:*

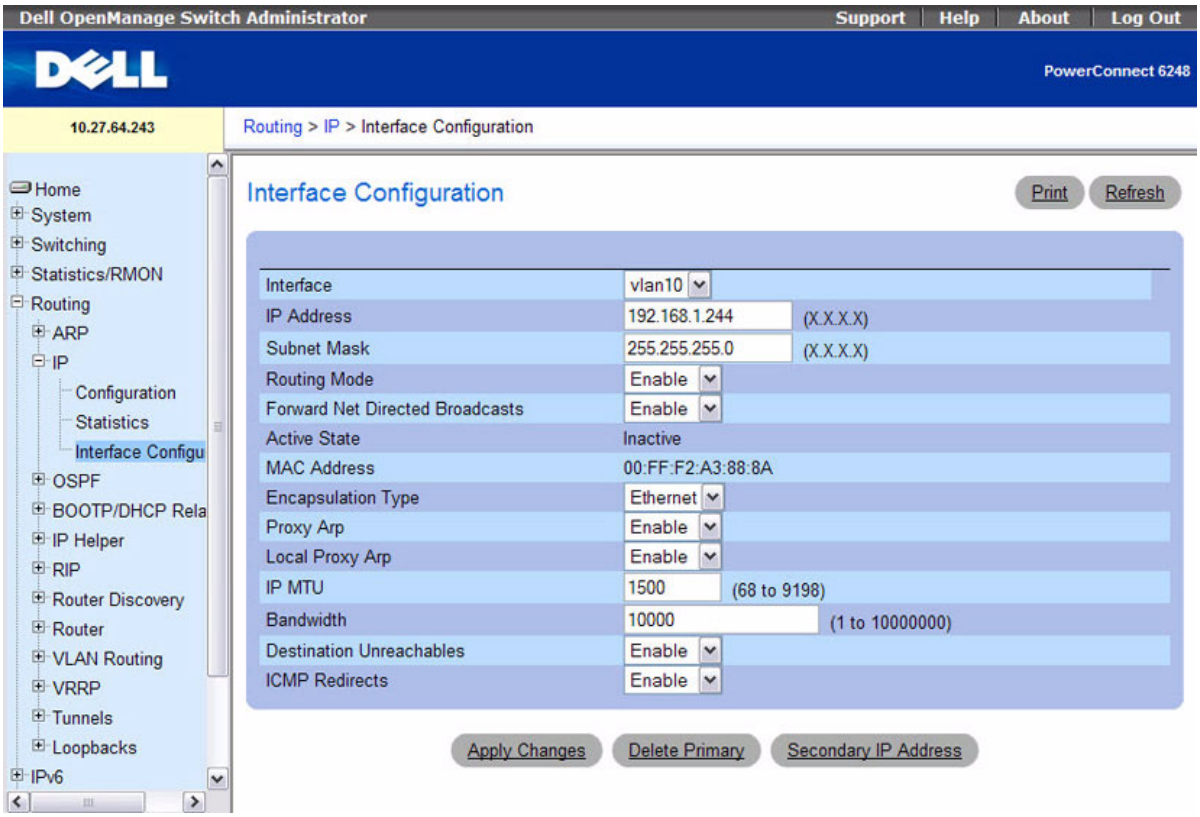
- IP Routing Commands

IP Interface Configuration

Use the **IP Interface Configuration** page to update IP interface data for this switch. The IP interface configuration includes the ability to configure the bandwidth, Destination Unreachable messages, and ICMP Redirect messages.

To display the page, click **Routing > IP > Interface Configuration** in the tree view.

Figure 9-5. IP Interface Configuration



Downloaded from www.Manualslib.com manuals search engine

The **IP Interface Configuration** page contains the following fields:

- **Interface** — Select the interface to configure from the drop-down menu. The drop-down menu contains loopback interfaces and VLANs created from the **Switching→VLAN→VLAN Membership→Add** page.
- **IP Address** — Enter the IP address for the interface.
- **Subnet Mask** — Enter the subnet mask for the interface. This is also referred to as the subnet/network mask, and defines the portion of the interface's IP address that is used to identify the attached network.
- **Routing Mode** — Setting this enables or disables routing for an interface. The default value is **Enable**.
- **Forward Net Directed Broadcasts** — Select how network directed broadcast packets should be handled. If you select **Enable** from the drop-down menu network directed broadcasts are forwarded. If you select **Disable** they are dropped. The default value is **Disable**.
- **Active State** — The state of the specified interface is either **Active** or **Inactive**. An interface is considered active if the link is up and it is in forwarding state.
- **MAC Address** — The burned-in physical address of the specified interface. The format is six two-digit hexadecimal numbers separated by colons, for example 00:06:29:32:81:40. This value is valid for physical interfaces. For logical interfaces, such as VLAN routing interfaces, the field displays the system MAC address.
- **Encapsulation Type** — Select the link layer encapsulation type for packets transmitted from the specified interface from the drop-down menu. The possible values are **Ethernet** and **SNAP**. The default is **Ethernet**.
- **Proxy ARP** — Select to **Disable** or **Enable** proxy ARP for the specified interface from the drop-down menu.
- **Local Proxy ARP** — Select to **Disable** or **Enable** Local Proxy ARP for the specified interface from the drop-down menu.
- **IP MTU** — Specifies the maximum transmission unit (MTU) size of IP packets sent on an interface. Valid range is (68 to 9198). The default value is 1500.
- **Bandwidth** — Specifies the configured bandwidth on this interface for the OSPF link cost calculation. This setting does not affect the actual speed of an interface, and the speed of the interface is communicated to higher level protocols. The valid range is (1 to 10000000).
- **Destination Unreachables** — Select Enable to allow the interface to generate ICMP Destination Unreachable messages on this interface. Select Disable to prevent the interface from generating ICMP Destination Unreachable messages on this interface. By default, the Destination Unreachables mode is Enable.
- **ICMP Redirects** — Select Enable to allow the interface to generate ICMP redirect messages. Select Disable to prevent the interface from generating ICMP redirect messages. The ICMP Redirect feature is also configurable globally. If the ICMP Redirect feature is enabled on the interface, it must be enabled globally in order for the interface to generate ICMP redirect messages.

Downloaded from www.Manualslib.com manuals search engine

Modifying an IP Interface

1. Open the **IP Interface Configuration** page.
2. Change values as needed.
3. Click **Apply Changes**.

   Changes are saved, and the IP Interface is updated.

IP Interface Configuration CLI Commands

For information about the CLI commands that perform this function, see the following chapters in the *CLI Reference Guide:*

- IP Addressing Commands
- IP Routing Commands
- ARP Commands

OSPF

The Open Shortest Path First (OSPF) routing protocol is an Interior Gateway Protocol (IGP). Every OSPF router builds a shortest path tree of all the routers and networks in the domain. Routing information is propagated in Link State Update packets both periodically and in the event of network topology changes. This information is received, assimilated and stored in the OSPF databases of individual routers. An integral piece of information in the database exchange is the number and IP Addresses of the interfaces that are associated with the router. OSPF treats secondary IP Addresses as stub networks attached to the router. Hence though these networks are advertised in the OSPF routing domain, neighbor adjacencies are never established on secondary addresses. It is also important to note here that all secondary IP Addresses must be in the same area as the primary IP Address so that they get advertised by OSPF. This is always true in the case of the PowerConnect M6220/M6348/M8024 software implementation because the area configuration is on a per interface basis as against a per network basis.

The **OSPF** menu page contains links to web pages that configure and display OSPF parameters and data. To display this page, click **Routing > OSPF** in the tree view. Following are the web pages accessible from this menu page:

- OSPF Configuration
- Area Configuration
- Stub Area Summary
- Area Range Configuration
- Interface Statistics
- Interface Configuration
- Neighbor Table
- Neighbor Configuration

Downloaded from www.Manualslib.com manuals search engine

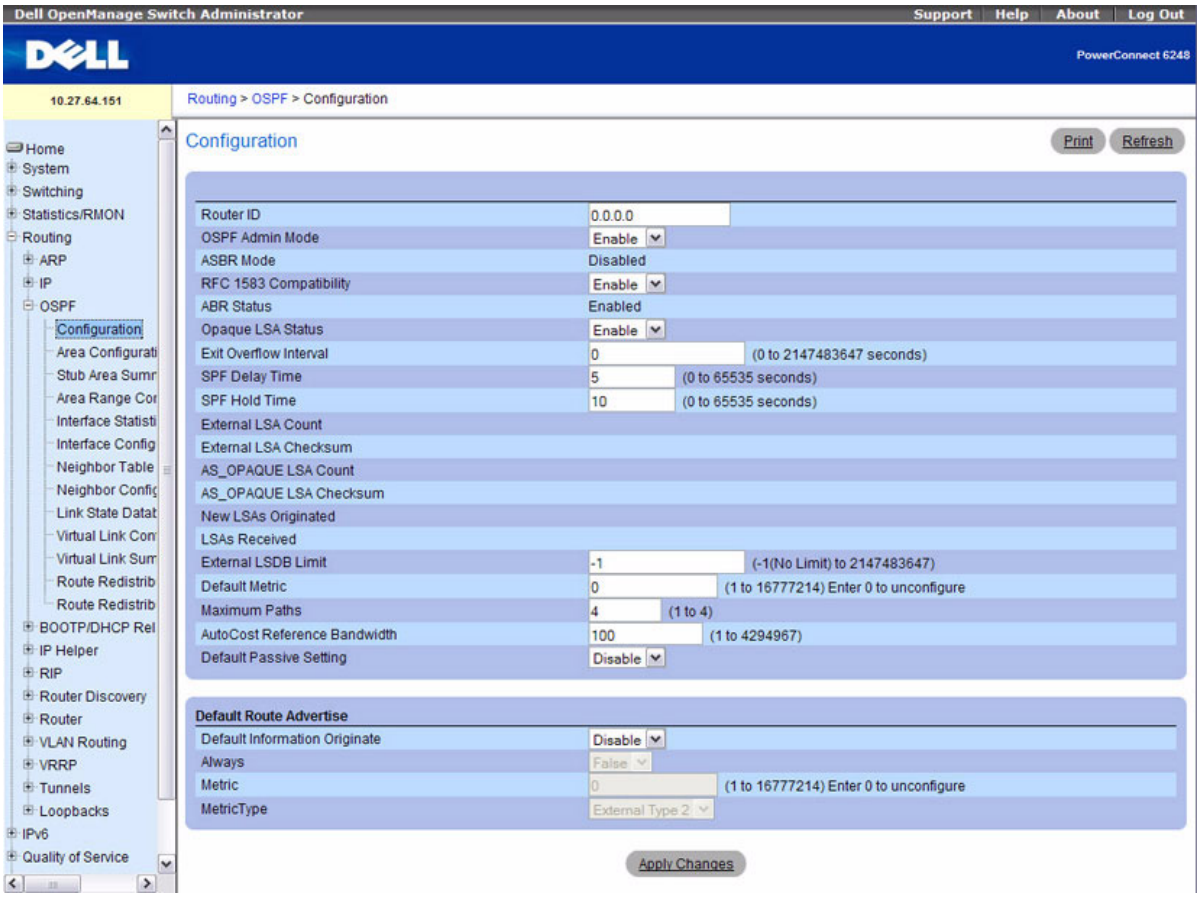
- Link State Database
- Virtual Link Configuration
- Virtual Link Summary
- Route Redistribution Configuration
- Route Redistribution Summary

OSPF Configuration

Use the **OSPF Configuration** page to enable OSPF on a router and to configure the related OSPF settings.

To display the page, click **Routing > OSPF > Configuration** in the tree view.

Figure 9-6. OSPF Configuration



Downloaded from www.Manualslib.com manuals search engine

The **OSPF Configuration** page contains the following fields:

- **Router ID** — The 32-bit integer in dotted decimal format that uniquely identifies the router within the autonomous system (AS). If you want to change the Router ID you must first disable OSPF. After you set the new Router ID, you must re-enable OSPF to have the change take effect. The default value is 0.0.0.0, although this is not a valid Router ID.
- **OSPF Admin Mode** — Select Enable or Disable from the drop-down menu. If you select Enable OSPF is activated for the switch. The default value is Disable. You must configure a Router ID before OSPF can become operational.

NOTE: Once OSPF is initialized on the router, it remains active until the router is reset.

- **ASBR Mode** — Reflects whether the ASBR mode is Enabled or Disabled. Enable implies that the router is an autonomous system border router. Router automatically becomes an ASBR when it is configured to redistribute routes learnt from other protocol.
- **RFC 1583 Compatibility** — Select Enable or Disable from the drop-down menu to specify the preference rules that are used when choosing among multiple AS-external-LSAs advertising the same destination. If you select Enable, the preference rules are those defined by RFC 1583. If you select Disable, the preference rules are those defined in Section 16.4.1 of the OSPF-2 standard (RFC 2328), which prevent routing loops when AS-external-LSAs for the same destination have been originated from different areas. The default value is Enable. To prevent routing loops, you should select Disable, but only if all OSPF routers in the routing domain are capable of operating according to RFC 2328.
- **ABR Status** — The values of this are Enabled or Disabled. Enabled implies that the router is an area border router. Disabled implies that it is not an area border router.
- **Opaque LSA Status** — Set this parameter to Enable if OSPF should store and flood opaque LSAs. An opaque LSA is used for flooding user-defined information within an OSPF router domain.
- **Exit Overflow Interval** — Enter the number of seconds that, after entering overflow state, the router should wait before attempting to leave overflow state. This allows the router to again originate non-default AS-external-LSAs. If you enter 0, the router does not leave Overflow State until restarted. The range is 0 to 2147483647 seconds.
- **SPF DelayTime** — Enter the number of seconds, Delay time (in seconds) is the time between when OSPF receives a topology change and when it starts an SPF calculation. It can be an integer from 0 to 65535. The default time is 5 seconds. A value of 0 means that there is no delay; that is, the SPF calculation is started immediately.
- **SPF HoldTime** — Enter the number of seconds, minimum time (in seconds) between two consecutive SPF calculations.It can be an integer from 0 to 65535. The default time is 10 seconds. A value of 0 means that there is no delay; that is, two SPF calculations can be done, one immediately after the other.
- **External LSA Count** — The number of external (LS type 5) LSAs (link state advertisements) in the link state database.

Downloaded from www.Manualslib.com manuals search engine

- **External LSA Checksum** — The sum of the LS checksums of the external LSAs (link state advertisements) contained in the link-state database. This sum can be used to determine if there has been a change in a router's link state database, and to compare the link-state databases of two routers. This value is in hexadecimal.
- **AS_OPAQUE LSA Count** — Shows the number of opaque LSAs with domain wide flooding scope.
- **AS_OPAQUE LSA Checksum** — Shows the sum of the LS checksums of the opaque LSAs with domain wide flooding scope. This sum can be used to determine if there has been a change in a router's link state database, and to compare the link-state databases of two routers. This value is in hexadecimal.
- **New LSAs Originated** — In any given OSPF area, a router originates several LSAs. Each router originates a router-LSA. If the router is also the Designated Router for any of the area's networks, it originates network-LSAs for those networks. This value represents the number of LSAs originated by this router.
- **LSAs Received** — The number of LSAs (link state advertisements) received that were determined to be new instantiations. This number does not include newer instantiations of self-originated LSAs.
- **External LSDB Limit** — The maximum number of AS-External-LSAs that can be stored in the database. A value of -1 implies there is no limit on the number that can be saved. The valid range of values is -1 to 2147483647.
- **Default Metric** — Sets a default for the metric of redistributed routes.This field displays the default metric if one has already been set or blank if not configured earlier. The valid values are 1 to 16777214. Enter 0 to unconfigure.
- **Maximum Paths** — Configure the maximum number of paths that OSPF can report to a given destination. The valid values are 1 to 4.
- **AutoCost Reference Bandwidth** — This field configures the value that OSPF uses in calculating the default metric for an interface. OSPF calculates the link cost of each interface as Cost = (Reference Bandwidth in Mbps) / (Interface Bandwidth). For example, setting this value to 1000 Mbps would cause all 1-Gbps interfaces to have a default cost of 1000/1000 = 1. For 100 Mbps interfaces, the default cost would be 1000/100 = 10.
- **Default Passive Setting** — Enable this setting to make all interfaces on the switch operate in passive mode passive. Configuring this field overwrites any present interface level passive mode setting. OSPF does not form adjacencies on passive interfaces, but it does advertise attached networks as stub networks. Interfaces are not passive by default. It is common to configure an OSPF interface to be passive when OSPF must advertise the subnets configured on the interface, but routers on the subnet belong to other OSPF domains, such as an OSPFv3 router at the end of a 6to4 tunnel.

Downloaded from www.Manualslib.com manuals search engine

Default Route Advertise

- **Default Information Originate** — Enable or Disable Default Route Advertise.
- **Always** — Sets the router advertise 0.0.0.0/0.0.0.0 when set to True.
- **Metric** — Specifies the metric of the default route. The valid values are 1 to 16777214. Enter 0 to unconfigure.
- **Metric Type** — Sets the metric type of the default route. Options are External Type 1 and External Type 2. External Type 2 is the default.

Modifying an OSPF Configuration

1. Open the **OSPF Configuration** page.
2. Change values as needed.
3. Click **Apply Changes**.

   Changes are saved, and the OSPF Interface is updated.

OSPF Configuration CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide:*

- OSPF Commands

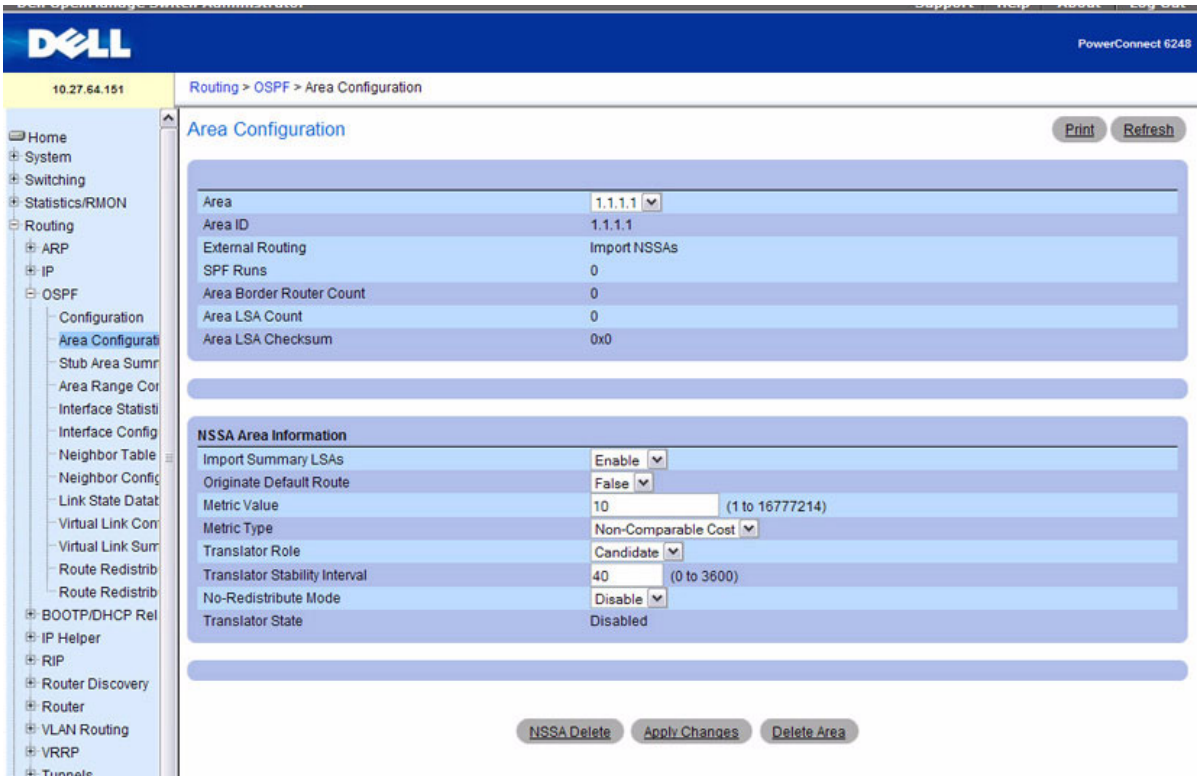
Area Configuration

The **OSPF Area Configuration** page lets you create a Stub area configuration and NSSA once you've enabled OSPF on an interface through **Routing > OSPF > Interface Configuration**. At least one router must have OSPF enabled for this web page to display.

To display the page, click **Routing > OSPF > Area Configuration** in the tree view. If a Stub Area has been created, the fields in the Stub Area Information are available. If a NSSA has been created, the fields in the NSSA Area Information are available.

Downloaded from www.Manualslib.com manuals search engine

Figure 9-7. OSPF Area Configuration



The **OSPF Area Configuration** page displays the following fields:

- **Area** — Select the area to be displayed from the drop-down menu. When an area is selected, fields in the Stub Area Information are displayed.
- **Area ID** — The OSPF area. An Area ID is a 32-bit integer in dotted decimal format that uniquely identifies the area to which a router interface connects.
- **External Routing** — A definition of the router's capabilities for the area, including whether or not AS-external-LSAs are flooded into/throughout the area. If the area is a stub area, then these are the possible options for which you may configure the external routing capability, otherwise the only option is Import External LSAs.
- **SPF Runs** — The number of times that the intra-area route table has been calculated using this area's link-state database. This is typically done using Dijkstra's algorithm.
- **Area Border Router Count** — The total number of area border routers reachable within this area. This is initially zero, and is calculated in each SPF Pass.
- **Area LSA Count** — The total number of link-state advertisements in this area's link-state database, excluding AS External LSAs.

Downloaded from www.Manualslib.com manuals search engine

- **Area LSA Checksum** — The 32-bit unsigned sum of the link-state advertisements' LS checksums contained in this area's link-state database. This sum excludes external (LS type 5) link-state advertisements. The sum can be used to determine if there has been a change in a router's link state database, and to compare the link-state database of two routers. This value is in hexadecimal.

Stub Area Information:

- **Import Summary LSAs** — Select Enable or Disable from the drop-down menu. If you select Enable summary LSAs is imported into stub areas.
- **Type of Service** — Specifies the parameters for the type of service requested. The parameters may be utilized by networks to define the handling of the datagram during transport The type of service is associated with the stub metric. The switch supports Normal only
- **Metric Value** — Enter the metric value you want applied for the default route advertised into the stub area. Valid values range from 1 to 16,777,215.

NSSA Area Information:

- **Import Summary LSAs** — Select Enable or Disable from the drop-down menu. If you select Enable summary LSAs is imported into stub areas.
- **Originate Default Route** —Enable or disable this field to set the default information origination configuration for the specified NSSA.
- **Metric Value** — Set the Metric value for NSSA. The valid range of values is (1 to 16777214).
- **Metric Type** — Select the type of metric specified in the Metric Value field, which can be one of the following:
  - **Default** — The default metric value.
  - **Comparable Cost** — External Type 1 metrics that are comparable to the OSPF metric.
  - **Non-comparable Cost** — External Type 2 metrics that are assumed be larger than the cost of the OSPF metric
- **Translator Role** — Configure the NSSA Translator Role as always/candidate.
- **Translator Stability Interval** — Configure the Translator Stability Interval for the selected NSSA.
- **No-Redistribute Mode** — Configure the route redistribution for the selected NSSA.
- **Translator State** — Displays the current state of the Translator.

Configuring an OSPF Area

1. Open the **OSPF Area Configuration** page.
2. Specify an area to configure.
3. Specify values in the remaining fields as needed.
4. Click **Apply Changes**.

   The OSPF area is defined and configured.

Downloaded from www.Manualslib.com manuals search engine

Displaying an OSPF Area Configuration

1. Open the **OSPF Area Configuration** page.
2. Select the OSPF area to display from the drop-down menu.

   The OSPF area configuration is displayed for this area.

Deleting an OSPF Area Configuration

Use these steps to delete NSSA configuration or Stub area configuration.

1. Open the **OSPF Area Configuration** page.
2. Select the OSPF area configuration to delete from the drop-down menu.

   The configuration displays.
3. Click **Delete**.

   The OSPF area configuration is removed.

Configuring OSPF Area CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide:*

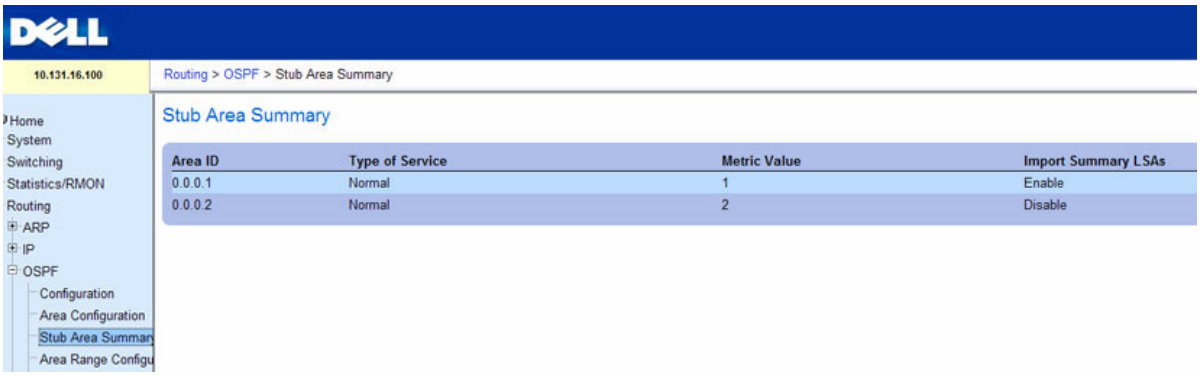
- OSPF Commands

Stub Area Summary

The **OSPF Stub Area Summary** page displays OSPF stub area detail.

To display the page, click **Routing > OSPF > Stub Area Summary** in the tree view.

Figure 9-8. OSPF Stub Area Summary



Downloaded from www.Manualslib.com manuals search engine

The **OSPF Stub Area Summary** page displays the following fields:

- **Area ID** — The Area ID of the stub area.
- **Type of Service** — The type of service associated with the stub metric. The switch supports **Normal** only.
- **Metric Value** — The metric value for the default route advertised into the area.
- **Import Summary LSAs** — Whether the import of Summary LASs is enabled or disabled.

Displaying OSPF Stub Area CLI Command

For information about the CLI command that performs this function, see the following chapter in the *CLI Reference Guide:*

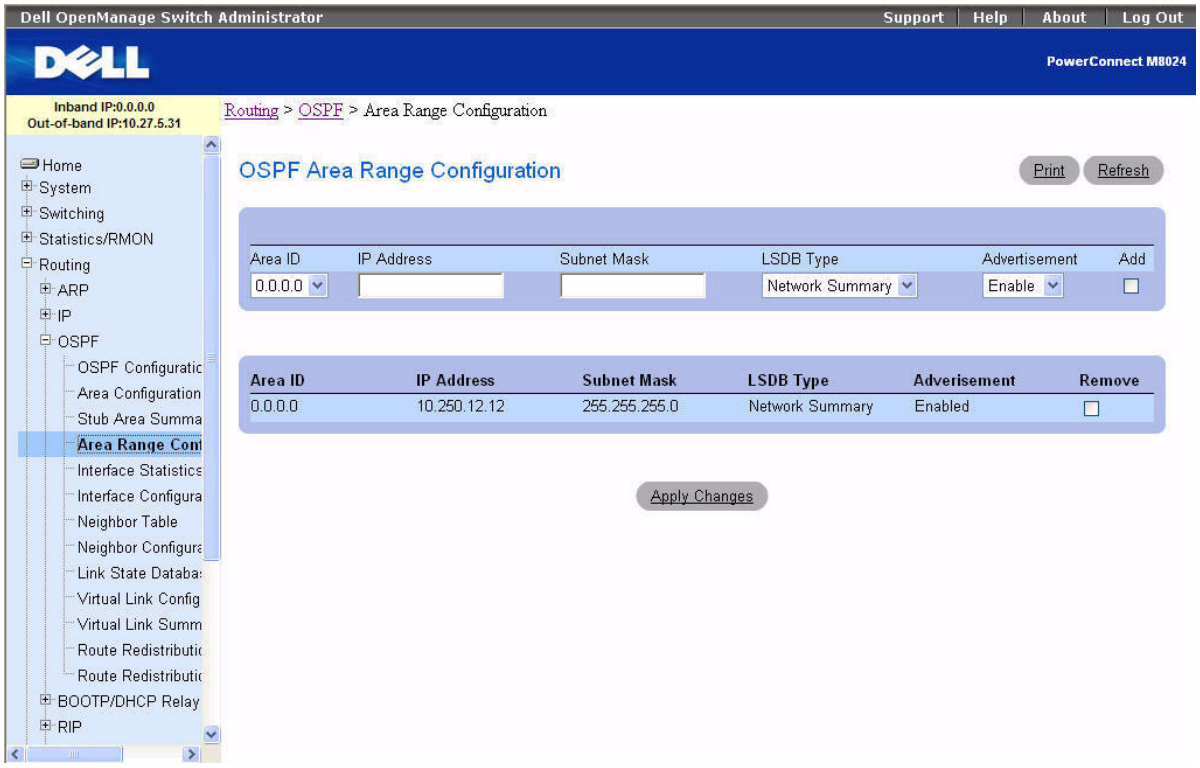
- OSPF Commands

Area Range Configuration

Use the **OSPF Area Range Configuration** page to configure and display an area range for a specified NSSA.

To display the page, click **Routing > OSPF > Area Range Configuration** in the tree view.

Figure 9-9. OSPF Area Range Configuration



Downloaded from www.Manualslib.com manuals search engine

The **OSPF Area Range Configuration** page contains the following fields:

- **Area ID** — Select the area for which data is to be configured from the drop-down menu.
- **IP Address** — Enter the IP Address for the address range for the selected area.
- **Subnet Mask** — Enter the Subnet Mask for the address range for the selected area.
- **LSDB Type** — Select the type of Link Advertisement associated with the specified area and address range. The default type is 'Network Summary.'
- **Advertisement** — Select Enable or Disable from the drop-down menu. If you selected Enable the address range is advertised outside the area through a Network Summary LSA. The default is Enable.
- **Add** — Check the Add check box if you wish to add an area range.

OSPF Area Range Table

- **Area ID** — Displays the OSPF area.
- **IP Address** — Displays the IP address of an address range for the area.
- **Subnet Mask** — Displays the subnet mask of an address range for the area.
- **LSDB Type** — Displays the link advertisement type for the address range and area.
- **Advertisement** — Displays the advertisement mode for the address range and area.
- **Remove** — Removes the specified area entry.

Defining an OSPF Area Range

1. Open the **OSPF Area Range Configuration** page.
2. Enter Area ID, IP Address, Subnet Mask, LSDB Type and Advertisement.
3. Click the **Add** check box.
4. Click **Apply Changes**.

   The OSPF area range is defined and configured. All configured OSPF area ranges are displayed in the table on the **OSPF Area Range Configuration** page.

Removing an OSPF Area Range Configuration

1. Open the **OSPF Area Range Configuration** page.
2. Select the **Remove** check box in the row of the **Area ID** to be deleted.
3. Click **Apply Changes**.

   The address range is removed from the area configuration.

OSPF Area Range Configuration CLI Command

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide:*

- OSPF Commands

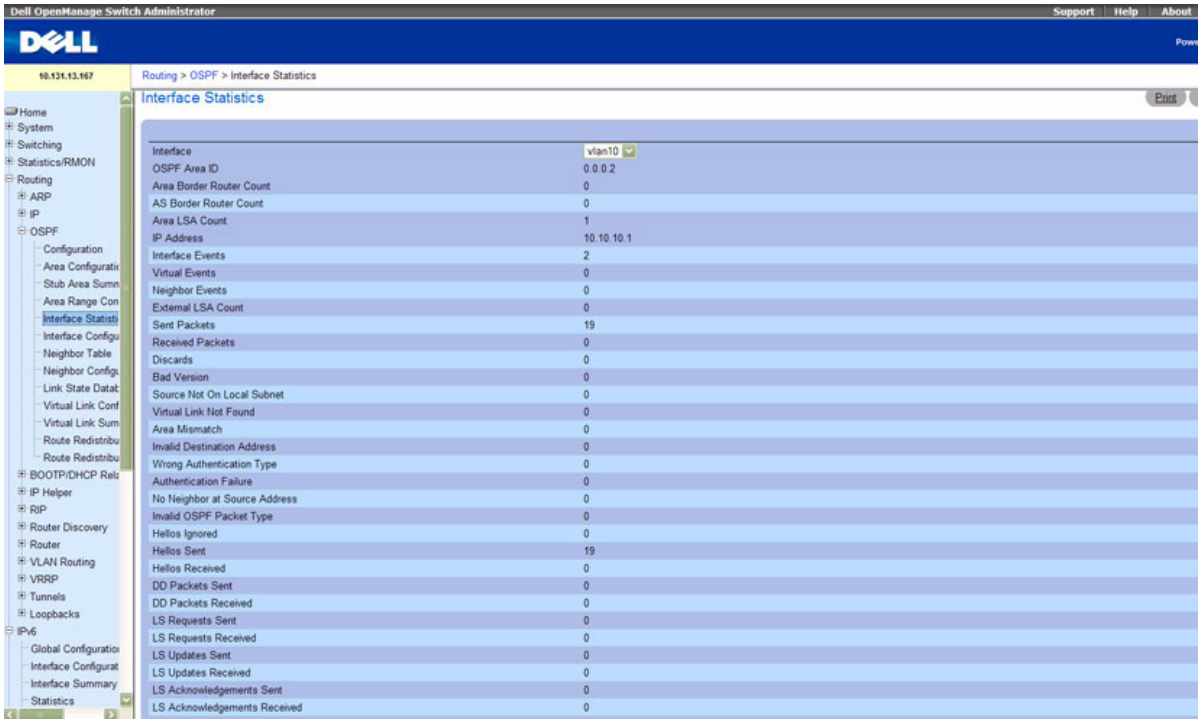
Downloaded from www.Manualslib.com manuals search engine

Interface Statistics

Use the **OSPF Interface Statistics** page to display statistics for the selected interface. The information is displayed only if OSPF is enabled.

To display the page, click **Routing > OSPF > Interface Statistics** in the tree view.

Figure 9-10. OSPF Interface Statistics



The **OSPF Interface Statistics** page contains the following fields:

- **Interface** — Select the interface for which data is to be displayed from the drop-down menu.
- **OSPF Area ID** — The OSPF area to which the selected router interface belongs. An OSPF Area ID is a 32-bit integer in dotted decimal format that uniquely identifies the area to which the interface connects.
- **Area Border Router Count** — The total number of area border routers reachable within this area. This is initially zero, and is calculated in each SPF Pass.
- **AS Border Router Count** — The total number of Autonomous System border routers reachable within this area. This is initially zero, and is calculated in each SPF Pass.
- **IP Address** — The IP address of the interface.
- **Interface Events** — The number of times the specified OSPF interface has changed its state, or an error has occurred.
- **Virtual Events** — The number of state changes or errors that have occurred on this virtual link.

Downloaded from www.Manualslib.com manuals search engine

- **Neighbor Events** — The number of times this neighbor relationship has changed state, or an error has occurred.
- **External LSA Count** — The number of external (LS type 5) link-state advertisements in the link-state database.
- **Sent Packets** — The number of OSPF packets transmitted on the interface.
- **Received Packets** — The number of valid OSPF packets received on the interface.
- **Discards** — The number of received OSPF packets discarded because of an error in the packet or an error in processing the packet.
- **Bad Version** — The number of received OSPF packets whose version field in the OSPF header does not match the version of the OSPF process handling the packet.
- **Source Not On Local Subnet** — The number of received packets discarded because the source IP address is not within a subnet configured on a local interface.
- **Virtual Link Not Found** — The number of received OSPF packets discarded where the ingress interface is in a non-backbone area and the OSPF header identifies the packet as belonging to the backbone, but OSPF does not have a virtual link to the packet's sender.
- **Area Mismatch** — The number of OSPF packets discarded because the area ID in the OSPF header is not the area ID configured on the ingress interface.
- **Invalid Destination Address** — The number of OSPF packets discarded because the packet's destination IP address is not the address of the ingress interface and is not the AllDrRouters or AllSpfRouters multicast addresses.
- **Wrong Authentication Type** — The number of packets discarded because the authentication type specified in the OSPF header does not match the authentication type configured on the ingress interface.
- **Authentication Failure** — The number of OSPF packets dropped because the sender is not an existing neighbor or the sender's IP address does not match the previously recorded IP address for that neighbor.
- **No Neighbor at Source Address** — The number of OSPF packets dropped because the sender is not an existing neighbor or the sender's IP address does not match the previously recorded IP address for that neighbor.
- **Invalid OSPF Packet Type** — The number of OSPF packets discarded because the packet type field in the OSPF header is not a known type.
- **Hellos Ignored** — The number of received Hello packets that were ignored by this router from the new neighbors after the limit has been reached for the number of neighbors on an interface or on the system as a whole.
- **Hellos Sent** — The number of Hello packets sent on this interface by this router.
- **Hellos Received** — The number of Hello packets received on this interface by this router.
- **DD Packets Sent** — The number of Database Description packets sent on this interface by this router.

Downloaded from www.Manualslib.com manuals search engine

- **DD Packets Received** — The number of Database Description packets received on this interface by this router.
- **LS Requests Sent** — The number of LS Requests sent on this interface by this router.
- **LS Requests Received** — The number of LS Requests received on this interface by this router.
- **LS Updates Sent** — The number of LS updates sent on this interface by this router.
- **LS Updates Received** — The number of LS updates received on this interface by this router.
- **LS Acknowledgements Sent** — The number of LS acknowledgements sent on this interface by this router.
- **LS Acknowledgements Received** — The number of LS acknowledgements received on this interface by this router.

Displaying OSPF Interface Statistics

1. Open the **OSPF Interface Statistics** page.
2. Select the interface for which data is to be displayed from the drop-down menu.

   Statistics for this interface display.

Displaying OSPF Interface Statistics using the CLI Command

For information about the CLI command that performs this function, see the following chapter in the *CLI Reference Guide:*

- OSPF Commands

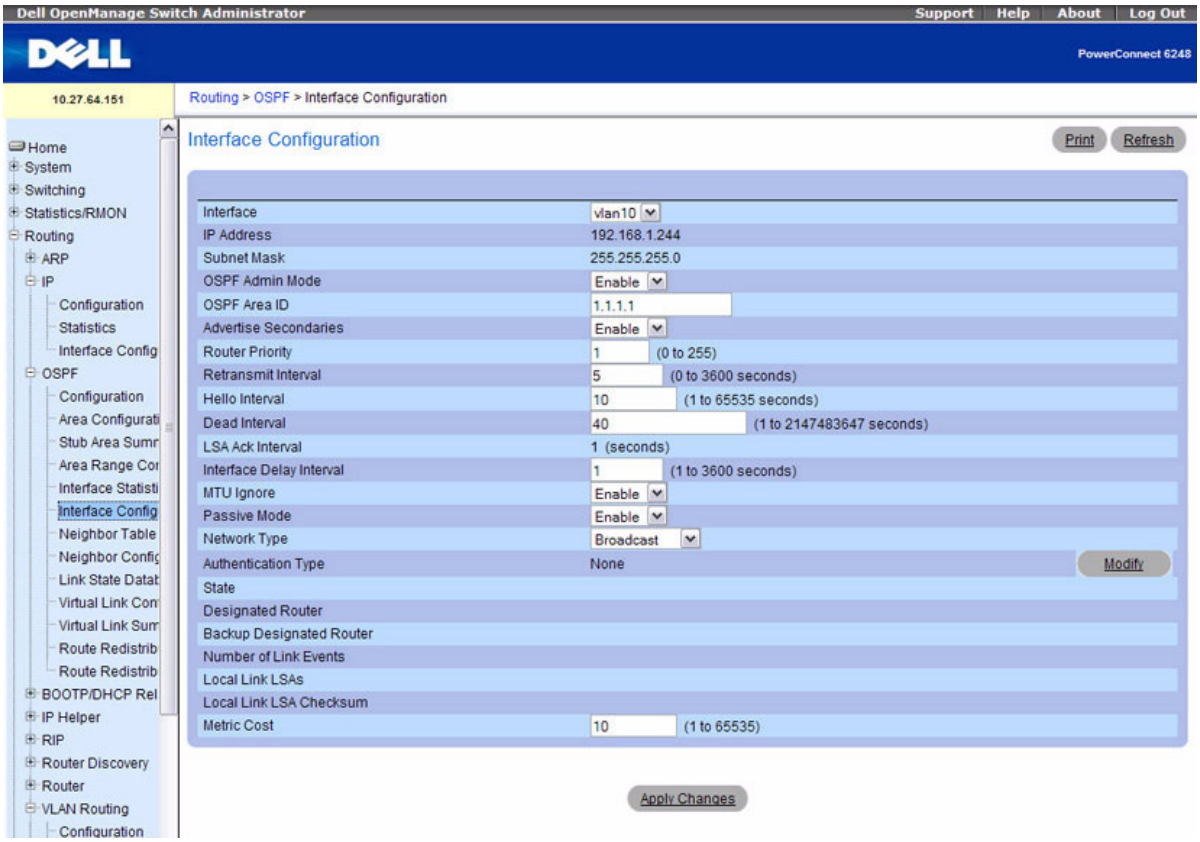
Interface Configuration

Use the **OSPF Interface Configuration** page to configure an OSPF interface.

To display the page, click **Routing > OSPF > Interface Configuration** in the tree view.

Downloaded from www.Manualslib.com manuals search engine

Figure 9-11. OSPF Interface Configuration



The **OSPF Interface Configuration** page contains the following fields:

- **Interface** — Select the interface for which data is to be displayed or configured from the drop-down menu.
- **IP Address** — Displays the address of the VLAN Interface.
- **Subnet Mask** — Displays the subnet mask of the VLAN Interface.
- **OSPF Admin Mode** — You may select **Enable** or **Disable** from the drop-down menu. The default value is **Disable**. You can configure OSPF parameters without enabling OSPF Admin Mode, but they have no effect until Admin Mode is enabled. The following information is displayed only if the Admin Mode is enabled: **State**, **Designated Router, Backup Designated Router**, **Number of Link Events**, **LSA Ack Interval**, and **Metric Cost**. For OSPF to be fully functional, you must enter a valid IP Address and Subnet Mask through the IP Interface Configuration page.

NOTE: Once OSPF is initialized on the router, it remains initialized until the router is reset.

- **OSPF Area ID** — Enter the 32-bit integer in dotted decimal format that uniquely identifies the OSPF area to which the selected router interface connects. If you assign an Area ID which does not exist, the area is created with default values.

Downloaded from www.Manualslib.com manuals search engine

- **Advertise Secondaries** — Select **Enable** or **Disable** from the drop-down menu to indicate the advertiseability of all secondary addresses. By default all the secondary addresses would be advertised on an interface enabled for OSPF.
- **Router Priority** — Enter the OSPF priority for the selected interface. The priority of an interface is specified as an integer from 0 to 255. The default is 1, which is the highest router priority. A value of 0 indicates that the router is not eligible to become the designated router on this network.
- **Retransmit Interval** — Enter the OSPF retransmit interval for the specified interface. This is the number of seconds between link-state advertisements for adjacencies belonging to this router interface. This value is also used when retransmitting database descriptions and link-state request packets. Valid values range from 0 to 3600 seconds (1 hour). The default is 5 seconds.
- **Hello Interval** — Enter the OSPF hello interval for the specified interface in seconds. This parameter must be the same for all routers attached to a network. Valid values range from 1 to 65,535. The default is 10 seconds.
- **Dead Interval** — Enter the OSPF dead interval for the specified interface in seconds. This specifies how long a router waits to see a neighbor router's Hello packets before declaring that the router is down. This parameter must be the same for all routers attached to a network. This value should a multiple of the Hello Interval (for example 4). Valid values range from 1 to 65535. The default is 40.
- **LSA Ack Interval** — The number of seconds between LSA Acknowledgment packet transmissions, which must be less than the Retransmit Interval.
- **Interface Delay Interval** — Enter the OSPF Transit Delay for the specified interface. This specifies the estimated number of seconds it takes to transmit a link state update packet over the selected interface. Valid values range from 1 to 3600 seconds (1 hour). The default value is 1 second.
- **MTU Ignore** — Disables OSPF MTU mismatch detection on receiving packets. The default value is Disable.
- **Passive Mode** — Enable this mode to make the interface passive to prevent OSPF from forming an adjacency on an interface. OSPF advertises networks attached to passive interfaces as stub networks. Interfaces are not passive by default. It is common to configure an OSPF interface to be passive when OSPF must advertise the subnets configured on the interface, but routers on the subnet belong to other OSPF domains, such as an OSPFv3 router at the end of a 6to4 tunnel.
- **Network Type** — Sets the OSPF network type on the interface to broadcast or point-to-point.
  - **Broadcast** — OSPF only selects a designated router and originates network LSAs for broadcast networks. The default network type for Ethernet interfaces is broadcast.
  - **Point-to-Point** — When there are only two routers on the network, OSPF can operate more efficiently by treating the network as a point-to-point network. For point-to-point networks, OSPF does not elect a designated router or generate a network link state advertisement (LSA). Both endpoints of the link must be configured to operate in point-to-point mode.

Downloaded from www.Manualslib.com manuals search engine

- **Authentication Type** — You may select an authentication type other than **None** by clicking on the **Modify** button. You then see a new web page, where you can select the authentication type from the drop-down menu. Possible values are:
  - **None** — This is the initial interface state. If you select this option from the drop-down menu on the second screen and click **Apply Changes**, you are returned to the first screen, and no authentication protocols are run.
  - **Simple** — If you select **Simple**, you are prompted to enter an authentication key. This key is included, in the clear, in the OSPF header of all packets sent on the network. All routers on the network must be configured with the same key.
  - **Encrypt** — If you select **Encrypt**, you are prompted to enter both an authentication key and an authentication ID. Encryption uses the MD5 Message-Digest algorithm. All routers on the network must be configured with the same key and ID.
- **AuthKey** — Enter the OSPF Authentication Key for the specified interface. If you do not choose to use authentication you will not be prompted to enter a key. If you choose 'simple' authentication you cannot use a key of more than 8 octets. If you choose 'encrypt' the key may be up to 16 octets long. The key value will only be displayed if you are logged on with Read/Write privileges, otherwise it will be displayed as asterisks.
- **AuthKeyID** — Enter the ID to be used for authentication. You will only be prompted to enter an ID when you select **Encrypt** as the authentication type. The ID is a number between 0 and 255, inclusive.
- **State** — If the OSPF admin mode is enabled, this field shows the current state of the selected router interface. If the OSPF admin mode is disabled, this field is blank. Possible values are:
  - **Down** — This is the initial interface state. In this state, the lower-level protocols have indicated that the interface is unusable. In this state, interface parameters are set to their initial values. All interface timers are disabled, and there are no adjacencies associated with the interface.
  - **Loopback** — In this state, the router's interface to the network is looped back either in hardware or software. The interface is unavailable for regular data traffic. However, it may still be desirable to gain information on the quality of this interface, either through sending ICMP pings to the interface or through something like a bit error test. For this reason, IP packets may still be addressed to an interface in Loopback state. To facilitate this, such interfaces are advertised in router- LSAs as single host routes, whose destination is the IP interface address.
  - **Waiting** — The router is trying to determine the identity of the (Backup) Designated Router for the network by monitoring received Hello Packets. The router is not allowed to elect a Backup Designated Router or a Designated Router until it transitions out of Waiting state. This prevents unnecessary changes of (Backup) Designated Router.
  - **Designated Router** — This router is itself the Designated Router on the attached network. Adjacencies are established to all other routers attached to the network. The router must also originate a network-LSA for the network node. The network- LSA contains links to all routers (including the Designated Router itself) attached to the network.

Downloaded from www.Manualslib.com manuals search engine

- **Backup Designated Router** — This router is the Backup Designated Router on the attached network. It is promoted to Designated Router if the present Designated Router fails. The router establishes adjacencies to all other routers attached to the network. The Backup Designated Router performs slightly different functions during the Flooding Procedure, as compared to the Designated Router.
- **Other Designated Router** — The interface is connected to a broadcast or NBMA network on which other routers have been selected to be the Designated Router and Backup Designated Router either. The router attempts to form adjacencies to both the Designated Router and the Backup Designated Router.

- **Designated Router** — The identity of the Designated Router for this network, in the view of the advertising router. The Designated Router is identified here by its router ID. The value 0.0.0.0 means that there is no Designated Router. This field is only displayed if the OSPF admin mode is enabled.
- **Backup Designated Router** — The identity of the Backup Designated Router for this network, in the view of the advertising router. The Backup Designated Router is identified here by its router ID. Set to 0.0.0.0 if there is no Backup Designated Router. This field is only displayed if the OSPF admin mode is enabled.
- **Number of Link Events** — This is the number of times the specified OSPF interface has changed its state. This field is only displayed if the OSPF admin mode is enabled.
- **Local Link LSAs** — The number of opaque LSAs whose flooding scope is the link on this interface.
- **Local Link LSA Checksum** — The sum of the checksums of local link LSAs for this link.
- **Metric Cost** — Enter the value on this interface for the cost TOS (type of service). The range for the metric cost is between 1 and 65,535. Metric Cost is only configurable/displayed if OSPF is initialized on the interface.

Configuring an OSPF Interface Configuration

1. Open the **OSPF Interface Configuration** page.
2. Specify an interface to configure.
3. Specify values in the remaining fields as needed.
4. Click **Apply Changes**.

   The OSPF interface is configured.

Displaying an OSPF Interface Configuration

1. Open the **OSPF Interface Configuration** page.
2. Select the VLAN interface for which data is to be displayed from the drop-down menu.

   Configuration data for this interface display.

Downloaded from www.Manualslib.com manuals search engine

Configuring an OSPF Interface using CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide:*

- OSPF Commands

Neighbor Table

Use the **OSPF Neighbor Table** page to display the OSPF neighbor table list. When a particular neighbor ID is specified, detailed information about a neighbor is given. The information below is only displayed if OSPF is enabled.

To display the page, click **Routing > OSPF > Neighbor Table** in the tree view.

Figure 9-12. OSPF Neighbor Table

Downloaded from www.Manualslib.com manuals search engine

The **OSPF Neighbor Table** page displays the following fields:

- **Interface** — Select the interface for which data is to be displayed from a drop-down menu.
- **Router ID** — A 32-bit integer in dotted decimal format representing the neighbor interface.
- **IP Address** — The IP address of the neighboring router's interface to the attached network. It is used as the destination IP address when protocol packets are sent as unicasts along this adjacency. Also used in router-LSAs as the Link ID for the attached network if the neighboring router is selected to be designated router. The Neighbor IP address is learned when Hello packets are received from the neighbor. For virtual links, the Neighbor IP address is learned during the routing table build process.
- **Neighbor Interface Index** — An interface identifying the neighbor interface index.

Displaying the OSPF Neighbor Table Using the CLI Command

For information about the CLI command that performs this function, see the following chapter in the *CLI Reference Guide:*

- OSPF Commands

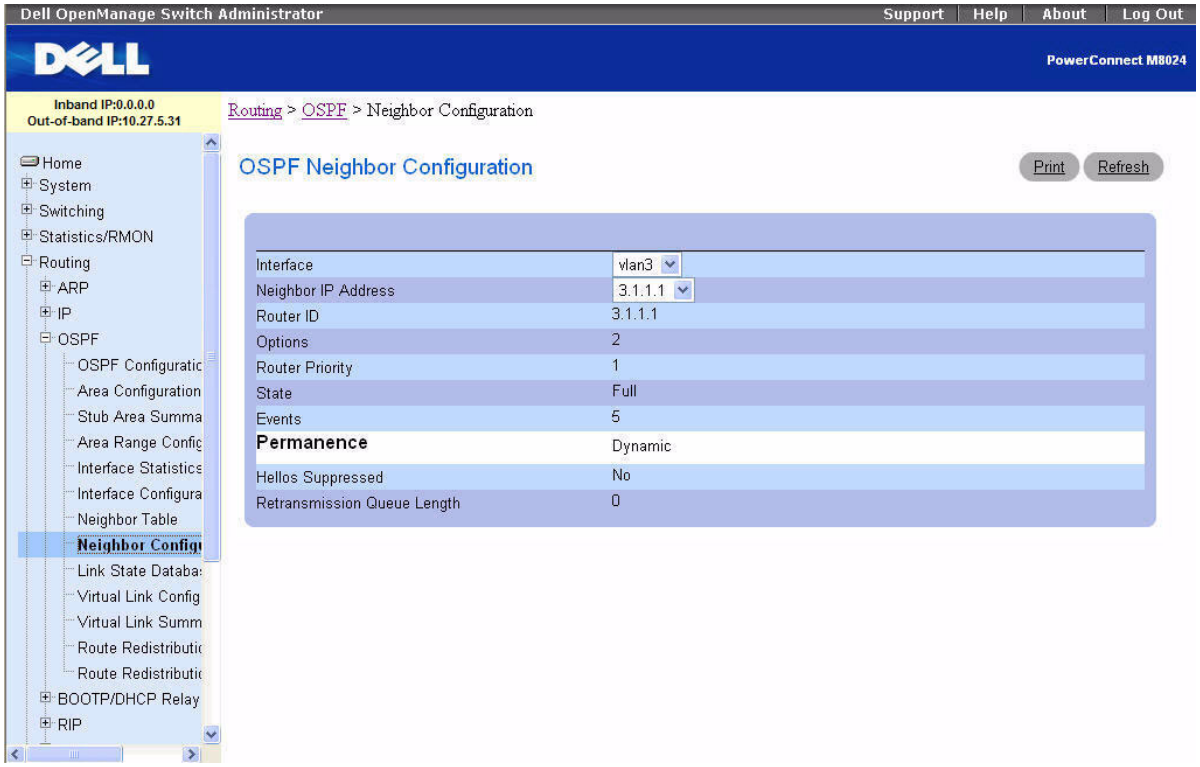
Neighbor Configuration

Use the **OSPF Neighbor Configuration** page to display the OSPF neighbor configuration for a selected neighbor ID. When a particular neighbor ID is specified, detailed information about a neighbor is given. The information below is only displayed if OSPF is enabled and the interface has a neighbor. The IP address is the IP address of the neighbor.

To display the page, click **Routing > OSPF > Neighbor Configuration** in the tree view.

Downloaded from www.Manualslib.com manuals search engine

Figure 9-13. OSPF Neighbor Configuration



The **OSPF Neighbor Configuration** page contains the following fields:

- **Interface** — Select the VLAN interface on which routing is enabled from the drop-down menu.
- **Neighbor IP Address** — Select the IP Address of the neighbor for which data is to be displayed.
- **Router ID** — A 32-bit integer in dotted decimal format that identifies the neighbor router.
- **Options** — The optional OSPF capabilities supported by the neighbor. The OSPF Options field is present in OSPF Hello packets, Database Description packets, and all link-state advertisements. The Options field enables OSPF routers to support (or not support) optional capabilities, and to communicate their capability level to other OSPF routers. Through this mechanism, routers of differing capabilities can be mixed within an OSPF routing domain. The Options value is a bitmap, and it signifies the capability of the neighbor.
- **Router Priority** — Displays the OSPF priority for the specified neighbor. The priority of a neighbor is a priority integer from 0 to 255. A value of 0 indicates that the router is not eligible to become the designated router on this network.
- **State** — The state of a neighbor can be the following:
  - **Down** — This is the initial state of a neighbor conversation. It indicates that there has been no recent information received from the neighbor. On NBMA networks, Hello packets may still be sent to Down neighbors, although at a reduced frequency.

Downloaded from www.Manualslib.com manuals search engine

- **Attempt** — This state is only valid for neighbors attached to NBMA networks. It indicates that no recent information has been received from the neighbor, but that an effort should be made to contact the neighbor (sending the neighbor Hello packets at intervals of Hello Interval).
- **Init** — In this state, a Hello packet has recently been seen from the neighbor. However, bidirectional communication has not yet been established with the neighbor (i.e., the router itself did not appear in the neighbor's Hello packet). All neighbors in this state (or greater) are listed in the Hello packets sent from the associated interface.
- **2-Way** — In this state, communication between the two routers is bidirectional. This has been assured by the operation of the Hello Protocol. This is the most advanced state short of beginning adjacency establishment. The (Backup) Designated Router is selected from the set of neighbors in state 2-Way or greater.
- **Exchange Start** — This is the first step in creating an adjacency between the two neighboring routers. The goal of this step is to decide which router is the master, and to decide upon the initial DD sequence number. Neighbor conversations in this state or greater are called adjacencies.
- **Exchange** — In this state, the router is describing its entire link state database by sending Database Description packets to the neighbor. In this state, Link State Request Packets may also be sent asking for the neighbor's more recent LSAs. All adjacencies in Exchange state or greater are used by the flooding procedure. These adjacencies are fully capable of transmitting and receiving all types of OSPF routing protocol packets.
- **Loading** — In this state, Link State Request packets are sent to the neighbor asking for the more recent LSAs that have been discovered (but not yet received) in the Exchange state.
- **Full** — In this state, the neighboring routers are fully adjacent. These adjacencies appear in router-LSAs and network-LSAs.

- **Events** — The number of times this neighbor relationship has changed state, or an error has occurred.
- **Permanence** — This variable displays the status of the entry. Dynamic and permanent see how the neighbor became known.
- **Hellos Suppressed** — This indicates whether Hellos are being suppressed to the neighbor.
- **Retransmission Queue Length** — The current length of the retransmission queue.

Displaying OSPF Neighbor Configuration

1. Open the **OSPF Neighbor Configuration** page.
2. Select the interface and the IP address to display.

   The neighbor configuration displays.

Displaying OSPF Neighbor Configuration using the CLI Command

For information about the CLI command that performs this function, see the following chapter in the *CLI Reference Guide:*

- OSPF Commands

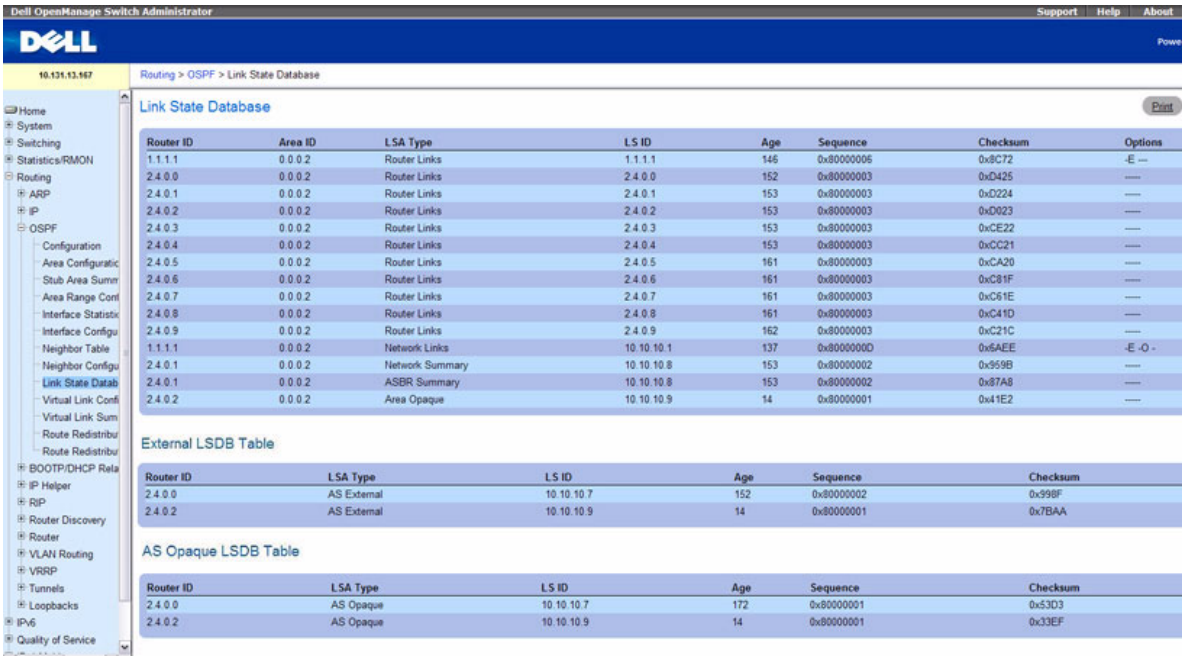
Downloaded from www.Manualslib.com manuals search engine

Link State Database

Use the **OSPF Link State Database** page to display OSPF link state, external LSDB table, and AS opaque LSDB table information.

To display the page, click **Routing > OSPF > Link State Database** in the tree view.

Figure 9-14. OSPF Link State Database



The **OSPF Link State Database** page displays the following fields:

- **Router ID** — The 32-bit integer in dotted decimal format that uniquely identifies the router within the autonomous system (AS). The Router ID is set on the IP Configuration page. If you want to change the Router ID you must first disable OSPF. After you set the new Router ID, you must re-enable OSPF to have the change take effect. The default value is 0.0.0.0, although this is not a valid Router ID.
- **Area ID** — The ID of an OSPF area to which one of the router interfaces is connected. An Area ID is a 32-bit integer in dotted decimal format that uniquely identifies the area to which an interface is connected.
- **LSA Type** — The format and function of the link state advertisement. Possible values are:
  - Router Links
  - Network Links
  - Network Summary
  - ASBR Summary
  - AS-external

Downloaded from www.Manualslib.com manuals search engine

- **LS ID** — The Link State ID identifies the piece of the routing domain that is being described by the advertisement. The value of the LS ID depends on the advertisement's LS type.
- **Age** — The time since the link state advertisement was first originated, in seconds.
- **Sequence** — The sequence number field is a signed 32-bit integer. It is used to detect old and duplicate link state advertisements. The larger the sequence number, the more recent the advertisement.
- **Checksum** — The checksum is used to detect data corruption of an advertisement. This corruption can occur while an advertisement is being flooded, or while it is being held in a router's memory. This field is the checksum of the complete contents of the advertisement, except the LS age field.
- **Options** — The Options field in the link state advertisement header indicates which optional capabilities are associated with the advertisement. Possible values are:
  - **Q** — This enables support for QoS Traffic Engineering.
  - **E** — This describes the way AS-external-LSAs are flooded.
  - **MC** — This describes the way IP multicast datagrams are forwarded according to the standard specifications.
  - **O** — This describes whether Opaque-LSAs are supported.
  - **V** — This describes whether OSPF++ extensions for VPN/COS are supported.

Virtual Link Configuration

Use the **Virtual Link Configuration** page to create or configure virtual interface information for a specific area and neighbor. A valid OSPF area must be configured before this page can be displayed.

To display the page, click **Routing > OSPF > Virtual Link Configuration** in the tree view.

Downloaded from www.Manualslib.com manuals search engine

Figure 9-15. OSPF Virtual Link Configuration - Create

The **OSPF Virtual Link Configuration** pages contain the following fields:

- **Virtual Link (Area ID - Neighbor Router ID)** — Select the virtual link for which you want to display or configure data. It consists of the Area ID and Neighbor Router ID. To create a new virtual link, select **Create New Virtual Link** from the drop-down menu to define a new virtual link. When **Create New Virtual Link** is selected, the following fields appear:
  - **Area ID** — The 32-bit integer in dotted decimal format that uniquely identifies the area to which a router interface connects.
  - Neighbor Router ID — The 32-bit integer in dotted decimal format that uniquely identifies the neighbor router that is part of the virtual link.
- **Hello Interval** — Enter the OSPF hello interval for the specified interface in seconds. This parameter must be the same for all routers attached to a network. Valid values range from 1 to 65535. The default is 10 seconds.
- **Dead Interval** — Enter the OSPF dead interval for the specified interface in seconds. This specifies how long a router waits to see a neighbor router's Hello packets before declaring that the router is down. This parameter must be the same for all routers attached to a network. This value should a multiple of the Hello Interval (for example, 4). Valid values range from 1 to 65535. The default is 40 seconds.

Downloaded from www.Manualslib.com manuals search engine

- **Interface Delay Interval (secs)** — The OSPF Transit Delay for the virtual link in units of seconds. It specifies the estimated number of seconds it takes to transmit a link state update packet over this interface.
- **State** — The current state of the selected Virtual Link. One of:
  - **Down** — This is the initial interface state. In this state, the lower-level protocols have indicated that the interface is unusable. In this state, interface parameters are set to their initial values. All interface timers are disabled, and there are no adjacencies associated with the interface.
  - **Waiting** — The router is trying to determine the identity of the (Backup) Designated Router by monitoring received Hello Packets. The router is not allowed to elect a Backup Designated Router or a Designated Router until it transitions out of Waiting state. This prevents unnecessary changes of (Backup) Designated Router.
  - **Point-to-Point** — The interface is operational, and is connected either to the virtual link. On entering this state the router attempts to form an adjacency with the neighboring router. Hello Packets are sent to the neighbor every HelloInterval seconds.
  - **Designated Router** — This router is itself the Designated Router on the attached network. Adjacencies are established to all other routers attached to the network. The router must also originate a network-LSA for the network node. The network- LSA contains links to all routers (including the Designated Router itself) attached to the network.
  - **Backup Designated Router** — This router is itself the Backup Designated Router on the attached network. It is promoted to Designated Router if the present Designated Router fails. The router establishes adjacencies to all other routers attached to the network. The Backup Designated Router performs slightly different functions during the Flooding Procedure, as compared to the Designated Router.
  - **Other Designated Router** — The interface is connected to a broadcast or NBMA network on which other routers have been selected to be the Designated Router and Backup Designated Router either. The router attempts to form adjacencies to both the Designated Router and the Backup Designated Router.
- **Neighbor State** — The state of the Virtual Neighbor Relationship.
- **Retransmit Interval** — Enter the OSPF retransmit interval for the specified interface. This is the number of seconds between link-state advertisements for adjacencies belonging to this router interface. This value is also used when retransmitting database descriptions and link-state request packets. Valid values range from 0 to 3600 seconds (1 hour). The default is 5 seconds.
- **Authentication Type** — You may select an authentication type other than none by clicking on the **Configure Authentication** button. You then see a new screen, where you can select the authentication type from the drop-down menu. The choices are:
  - **None** — This is the initial interface state. If you select this option from the drop-down menu on the second screen and click **Apply Changes,** you are returned to the first screen.

Downloaded from www.Manualslib.com manuals search engine

- **Simple** — If you select Simple you are prompted to enter an authentication key. This key is included, in the clear, in the OSPF header of all packets sent on the network. All routers on the network must be configured with the same key.
- **Encrypt** — If you select Encrypt you are prompted to enter both an authentication key and an authentication ID. Encryption uses the MD5 Message-Digest algorithm. All routers on the network must be configured with the same key and ID.

- **Authentication Key** — Enter the OSPF Authentication Key for the specified interface. If you do not choose to use authentication you are not prompted to enter a key. If you choose Simple authentication you cannot use a key of more than 8 characters. If you choose Encrypt the key may be up to 16 characters long. The key value is only displayed if you are logged on with Read/Write privileges, otherwise it is displayed as asterisks.
- **Authentication ID** — Enter the ID to be used for authentication. You are only prompted to enter an ID when you select Encrypt as the authentication type. The ID is a number between 0 and 255, inclusive.

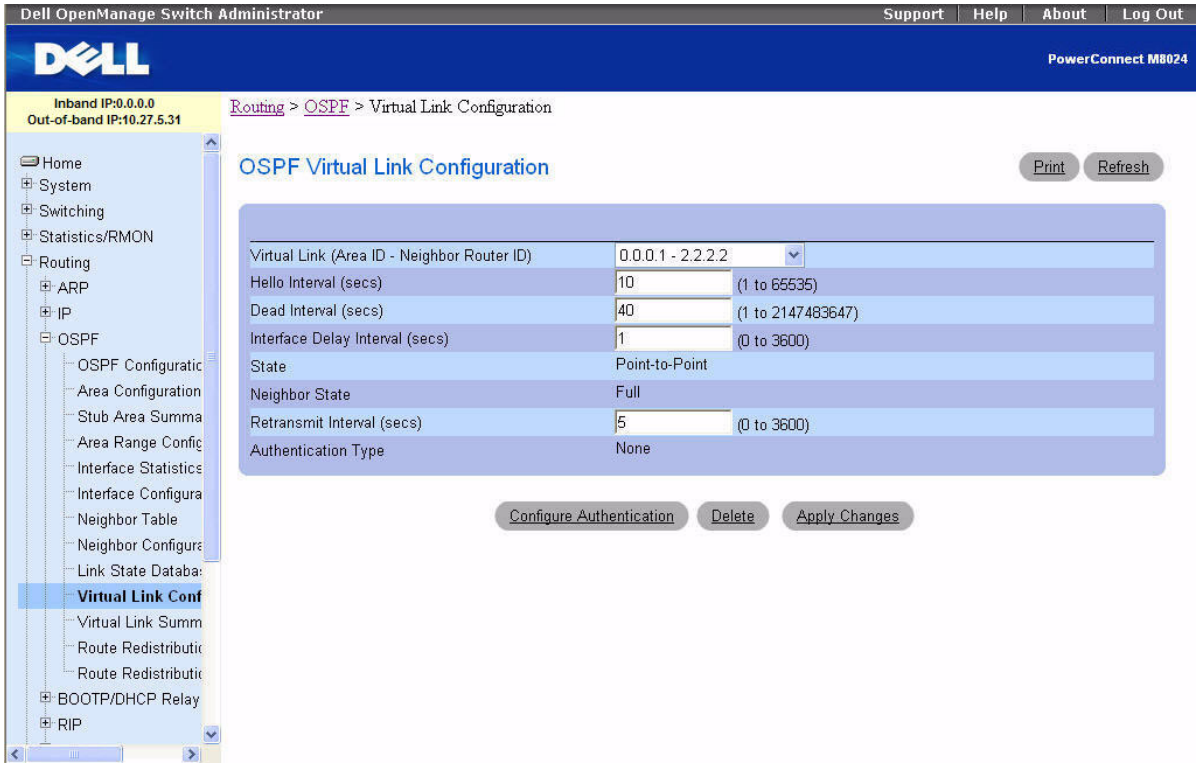
Defining a New Virtual Link

1. Open the **OSPF Virtual Link Configuration** page.
2. Select **Create New Virtual Link** from the **Virtual Link (Area ID - Neighbor Router ID)** drop-down menu.
3. Specify the neighbor router ID for the new virtual link.
4. Click **Apply Changes**.

   The remaining fields display when the Virtual Link is created.

Downloaded from www.Manualslib.com manuals search engine

Figure 9-16. OSPF Virtual Link Configuration

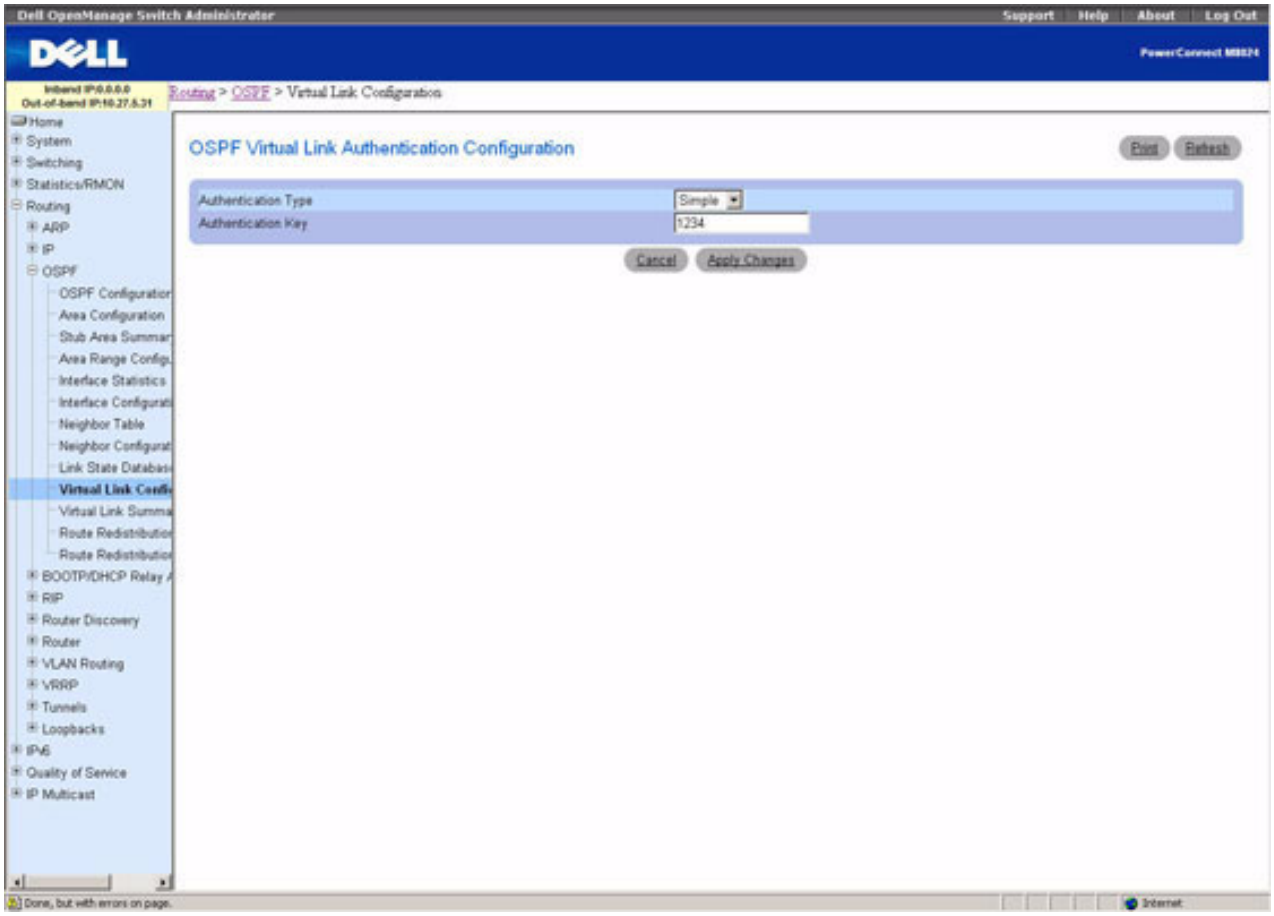


5. Click **Configure Authentication** to modify authentication.

   The following page appears:

Downloaded from www.Manualslib.com manuals search engine

Figure 9-17. OSPF Virtual Link Authentication Configuration



6. Select values for **Authentication Type** and **Authentication Key**.
7. Click **Apply Changes** when finished.

Configuring Virtual Link Data

1. Open the **OSPF Virtual Link Configuration** page.
2. Specify the area ID and neighbor router ID to configure.
3. Enter data into the fields as needed.
4. Click **Configure Authentication** to modify authentication.
5. Click **Apply Changes** when finished.

   The virtual link data for the specified IDs is configured, and the device is updated.

Downloaded from www.Manualslib.com manuals search engine

Displaying Virtual Link Data

1. Open the **OSPF Virtual Link Configuration** page.
2. Specify the area ID and neighbor router ID to display.

   The virtual link data for these IDs displays.

Removing a Virtual Link

1. Open the **OSPF Virtual Link Configuration** page.
2. Specify the Area ID and Neighbor Router ID associated with the virtual link to be removed.

   The related virtual link data displays.
3. Click **Delete**.

   The virtual link is removed, and the device is updated.

Configuring Virtual Link Data using the CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide:*

- OSPF Commands

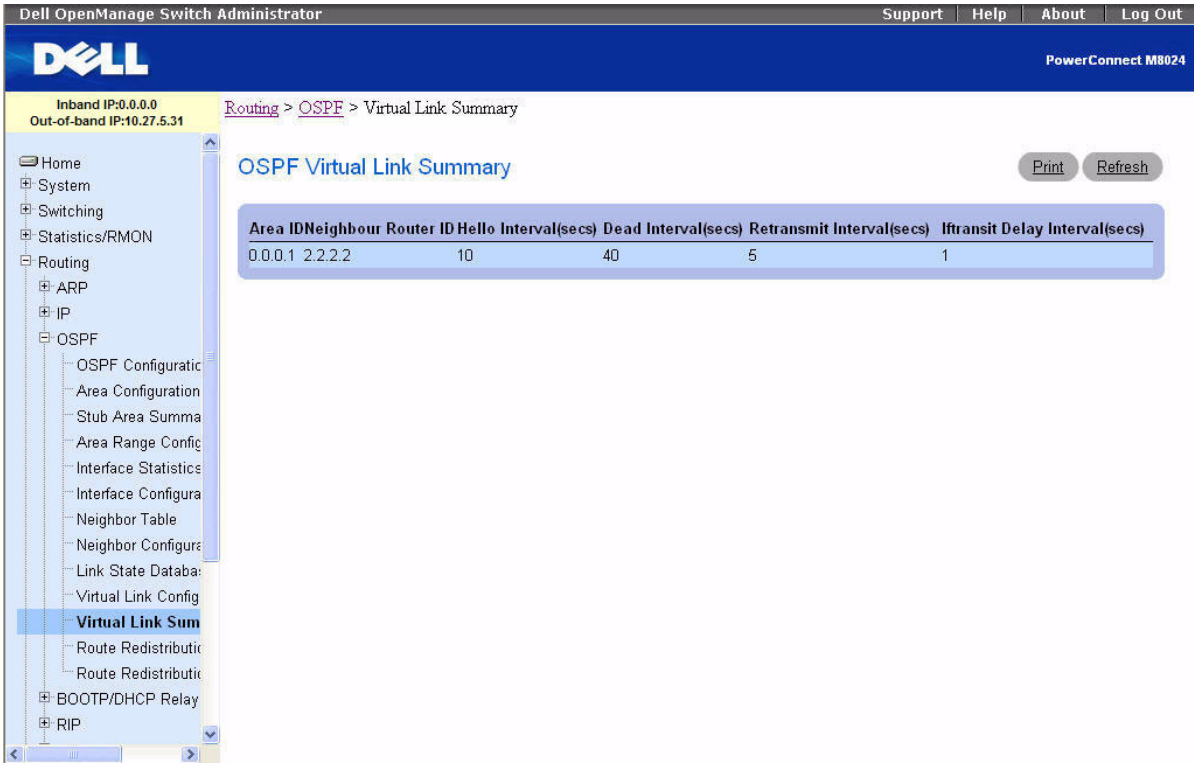
Virtual Link Summary

Use the **OSPF Virtual Link Summary** page to display all of the configured virtual links.

To display the page, click **Routing > OSPF > Virtual Link Summary** in the tree view.

Downloaded from www.Manualslib.com manuals search engine

Figure 9-18. OSPF Virtual Link Summary



The **OSPF Virtual Link Summary** page contains the following fields:

- **Area ID** — The Area ID portion of the virtual link identification for which data is to be displayed. The Area ID and Neighbor Router ID together define a virtual link.
- **Neighbor Router ID** — The neighbor portion of the virtual link identification. Virtual links may be configured between any pair of area border routers with interfaces to a common (non-backbone) area.
- **Hello Interval (secs)** — The OSPF hello interval for the virtual link in units of seconds. The value for hello interval must be the same for all routers attached to a network.
- **Dead Interval (secs)** — The OSPF dead interval for the virtual link in units of seconds. This specifies how long a router waits to see a neighbor router's Hello packets before declaring that the router is down. This parameter must be the same for all routers attached to a common network, and should be a multiple of the Hello Interval (i.e. 4).
- **Retransmit Interval (secs)** — The OSPF retransmit interval for the virtual link in units of seconds. This specifies the time between link-state advertisements for adjacencies belonging to this router interface. This value is also used when retransmitting database descriptions and link-state request packets.
- **Iftransit Delay Interval (secs)** — The OSPF Transit Delay for the virtual link in units of seconds. It specifies the estimated number of seconds it takes to transmit a link state update packet over this interface.

Downloaded from www.Manualslib.com manuals search engine

Displaying the Virtual Link Summary using the CLI Command

For information about the CLI command that performs this function, see the following chapter in the *CLI Reference Guide:*

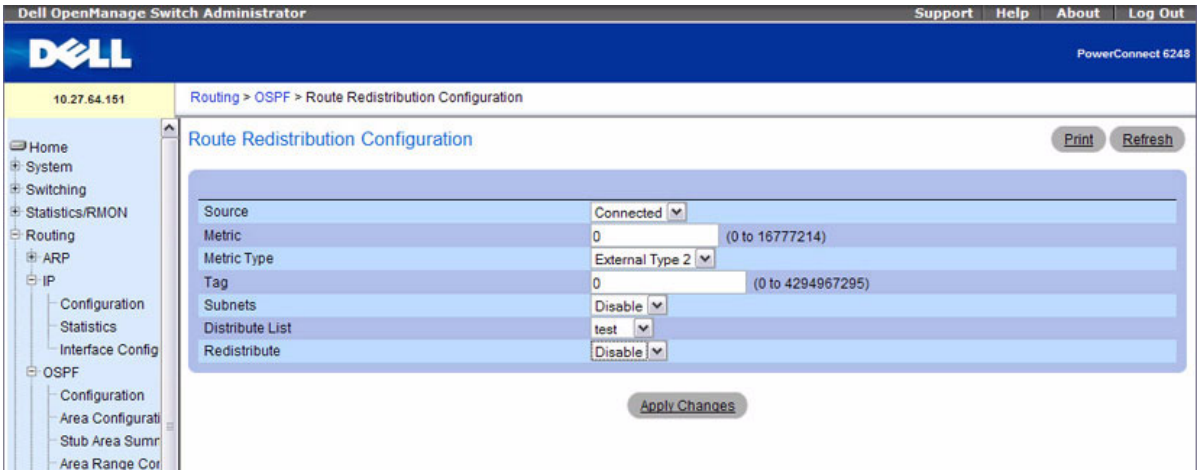
- OSPF Commands

Route Redistribution Configuration

Use the **OSPF Route Redistribution Configuration** page to configure redistribution in OSPF for routes learned through various protocols. You can choose to redistribute routes learned from all available protocols or from selected ones.

To display the page, click **Routing > OSPF > Route Redistribution Configuration** in the tree view.

Figure 9-19. OSPF Route Redistribution Configuration



Downloaded from www.Manualslib.com manuals search engine

The **OSPF Route Redistribution Configuration** page contains the following fields:

- **Source** — A protocol configured for OSPF to redistribute the routes learned through this protocol. Only source routes that have been configured for redistribution by OSPF are available. Possible values are Static, Connected, and RIP.
- **Metric** — Sets the metric value for redistributed routes. This field displays a metric value if the source was preconfigured. The valid values are 0 to 16777214.
- **Metric Type** — Select the OSPF metric type of redistributed routes from the drop-down menu.
- **Tag** — Sets the tag field in routes redistributed. This field displays a tag value if the source was preconfigured, otherwise 0 is displayed. The valid values are 0 to 4294967295.
- **Subnets** — Select whether the subnetted routes should be redistributed or not from the drop-down menu.
- **Distribute List** — Selects the Access List that filters the routes to be redistributed by the destination protocol. Only permitted routes are redistributed. If this command refers to a non-existent access list, all routes are permitted. The drop-down menu lists the ACLs configured from the **Switching→ Network Security→Access Control Lists→IP Access Control Lists** pages. When used for route filtering, the only fields in an access list that get used are:
  - Source IP Address and netmask
  - Destination IP Address and netmask
  - Action (permit or deny)

  All other fields (source and destination port, precedence, tos, and so on.) are ignored.

  The source IP address is compared to the destination IP address of the route. The source IP netmask in the access list rule is treated as a wildcard mask, indicating which bits in the source IP address must match the destination address of the route.

  Note: A 1 in the mask indicates a Don't Care in the corresponding address bit.

  When an access list rule includes a destination IP address and netmask (an extended access list), the destination IP address is compared to the network mask of the route destination. The destination netmask in the access list serves as a wildcard mask, indicating which bits in the route's destination mask are significant for the filtering operation.
- **Redistribute** — Enables or disables the redistribution for the selected source protocol. This field has to be enabled in order to be able to configure any of the route redistribution attributes.

Downloaded from www.Manualslib.com manuals search engine

Creating an OSPF Route Redistribution Source

When no redistributions are configured, the system displays only Create in the Configured Source field and possible sources in the Available Source fields. When you select an Available Source, enter configuration data, and click **Apply Changes**, the item displays in the Configure Source drop-down list and is removed from the Available Source drop-down list.

1. Open the **OSPF Route Redistribution Configuration** page.
2. Specify **Create** in the Configured Source field.
3. Select Static, Connected, or RIP from the Available Source field.
4. Click **Apply Changes** when finished.

   The route redistribution data is configured, and the device is updated.

Modifying OSPF Route Redistribution Data

1. Open the **OSPF Route Redistribution Configuration** page.
2. Select a source from the Configured Source drop-down.
3. Enter data in the fields as needed.
4. Click **Apply Changes** when finished.

   The route redistrbution data is configured, and the device is updated.

Configuring OSPF Route Redistribution Data using CLI Command

For information about the CLI command that performs this function, see the following chapter in the *CLI Reference Guide:*

- OSPF Commands

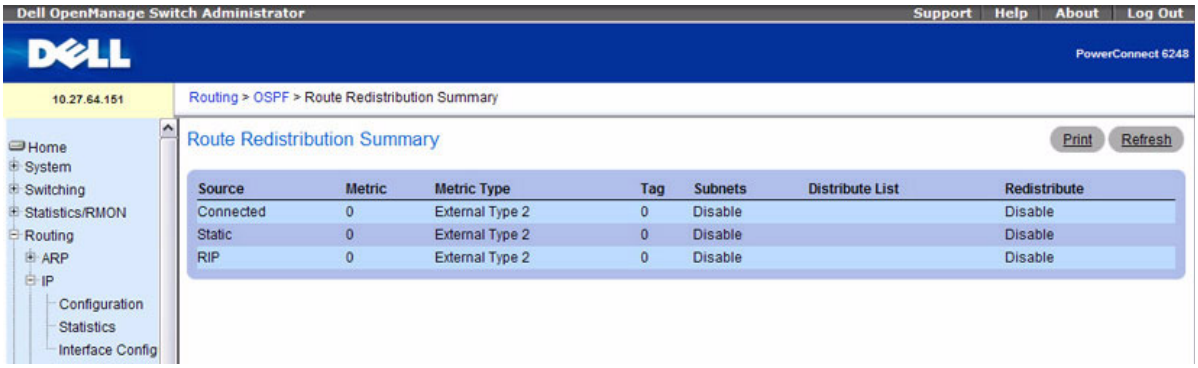
Downloaded from www.Manualslib.com manuals search engine

Route Redistribution Summary

Use the **OSPF Route Redistribution Summary** page to display OSPF Route Redistribution configurations.

To display the page, click **Routing > OSPF > Route Redistribution Summary** in the tree view.

Figure 9-20. OSPF Route Redistribution Summary



The **OSPF Route Redistribution Summary** page contains the following fields:

- **Source** — The Source Route to be redistributed by OSPF.
- **Redistribute** — Specify whether to allow the routes learned through this protocol to be redistributed.
- **Metric** — The Metric of redistributed routes for the given Source Route. Displays 0 when not configured.
- **Metric Type** — The OSPF metric type of redistributed routes.
- **Tag** — The tag field in routes redistributed. This field displays the tag value if the source was preconfigured, otherwise 0 is displayed.
- **Subnets** — Specify whether the subnetted routes should be redistributed (**Enable**) or not (**Disable**).
- **Distribute List** — The access list that filters the routes to be redistributed by the destination protocol. Displays 0 when not configured.
- **Redistribute** — Redistribute among other VLANs in the domain.

Displaying the Route Redistribution Summary using the CLI Command

For information about the CLI command that performs this function, see the following chapter in the *CLI Reference Guide:*

- OSPF Commands

Downloaded from www.Manualslib.com manuals search engine

BOOTP/DHCP Relay Agent

BootP/DHCP Relay Agent enables BootP/DHCP clients and servers to exchange BootP/DHCP messages across different subnets. The relay agent receives the requests from the clients, and checks the valid hops and giaddr fields. If the number of hops is greater than the configured, the agent assumes the packet is looped through the agents and discards the packet. If giaddr field is zero the agent must fill in this field with the IP address of the interface on which the request was received. The agent unicasts the valid packets to the next configured destination. The server responds with a unicast BOOTREPLY addressed to the relay agent closest to the client as indicated by giaddr field. Upon reception of the BOOTREPLY from the server, the agent forwards this reply as broadcast or unicast on the interface form where the BOOTREQUEST was arrived. This interface can be identified by giaddr field.

The PowerConnect M6220/M6348/M8024 DHCP component also supports DHCP relay agent options to identify the source circuit when customers are connected to the Internet with high-speed modem. The relay agent inserts these options when forwarding the request to the server and removes them when sending the reply to the clients.

If an interface has more than one IP address, the relay agent should use the primary IP address configured as its relay agent IP address.

The **BOOTP/DHCP Relay Agent** menu page contains links to web pages that configure and display BOOTP/DHCP relay agent. To display this page, click **Routing > BOOTP/DHCP Relay Agent** in the tree view. Following are the web pages accessible from this menu page:

- BOOTP/DHCP Relay Agent Configuration
- BOOTP/DHCP Relay Agent Status

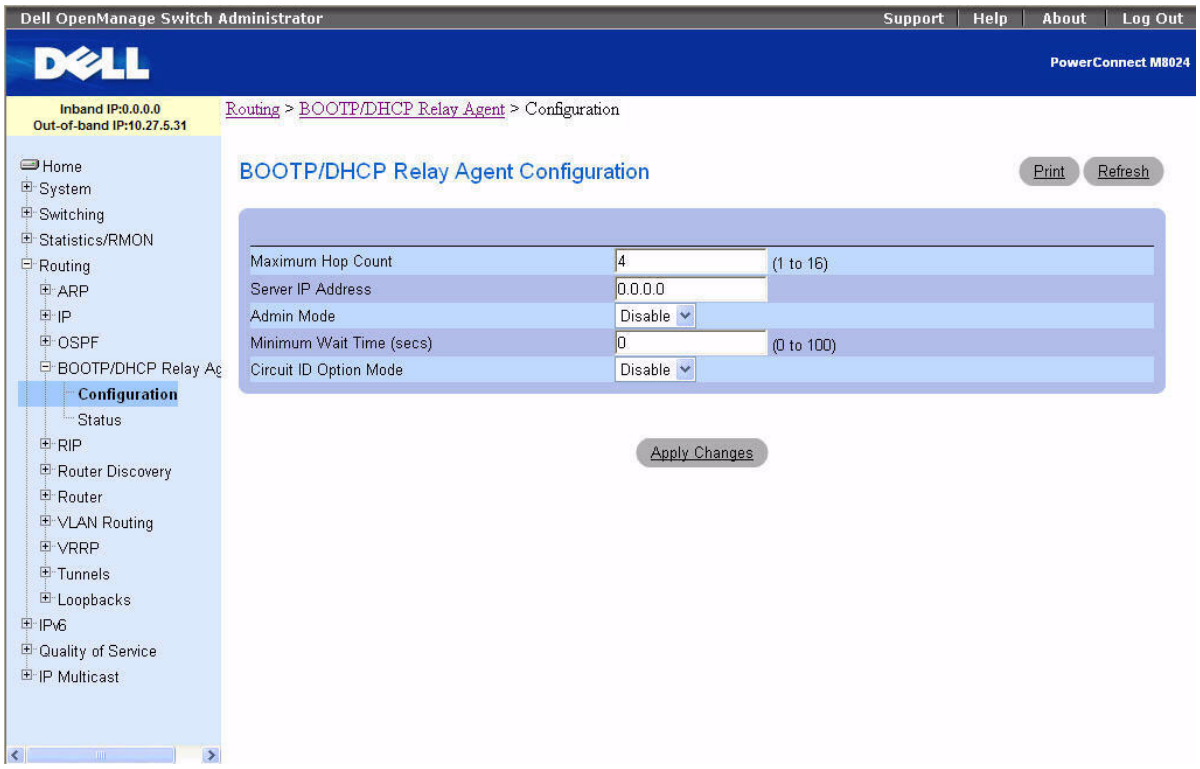
Downloaded from www.Manualslib.com manuals search engine

BOOTP/DHCP Relay Agent Configuration

Use the **BOOTP/DHCP Relay Agent Configuration** page to configure and display a BOOTP/DHCP relay agent.

To display the page, click **Routing > BOOTP/DHCP Relay Agent > Configuration** in the tree view.

Figure 9-21. BOOTP/DHCP Relay Agent Configuration



The **BOOTP/DHCP Relay Agent Configuration** page contains the following fields:

- **Maximum Hop Count** — Enter the maximum number of hops a client request can take before being discarded.
- **Server IP Address** — Enter either the IP address of the BOOTP/DHCP server or the IP address of the next BOOTP/DHCP Relay Agent.
- **Admin Mode** — Select Enable or Disable from the drop-down menu. When you select Enable, BOOTP/DHCP requests are forwarded to the IP address you entered in the Server IP address field.
- **Minimum Wait Time (secs)** — Enter a time in seconds. This value is compared to the time stamp in the client's request packets, which should represent the time since the client was powered up. Packets are only forwarded when the time stamp exceeds the minimum wait time.
- **Circuit ID Option Mode** — Select Enable or Disable from the drop-down menu. If you select Enable, the relay agent adds Option 82 header packets to the DHCP Request packets before forwarding them to the server, and strips them off while forwarding the responses to the client.

Downloaded from www.Manualslib.com manuals search engine

Configuring BOOTP/DHCP

1. Open the **BOOTP/DHCP Configuration** page.
2. Enter data in the fields as needed.
3. Click **Apply Changes** when finished.

   The BOOTP/DHCP data is configured, and the device is updated.

Configuring BOOTP/DHCP using CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide:*

- DHCP and BOOTP Relay Commands

BOOTP/DHCP Relay Agent Status

Use the **BOOTP/DHCP Relay Agent Status** page to display the BOOTP/DHCP Relay Agent configuration and status information.

To display the page, click **Routing > BOOTP/DHCP Relay Agent > Status** in the tree view.

Figure 9-22. BOOTP/DHCP Relay Agent Status

Downloaded from www.Manualslib.com manuals search engine

The **BOOTP/DHCP Status** page displays the following fields:

- **Maximum Hop Count** — The maximum number of Hops a client request can go without being discarded.
- **Server IP Address** — The IP address of the BOOTP/DHCP server or the IP address of the next BOOTP/DHCP Relay Agent.
- **Admin Mode** — The administrative mode of the relay. When you select Enable on the configuration page, BOOTP/DHCP requests are forwarded to the IP address you entered in the Server IP address field.
- **Minimum Wait Time (secs)** — The Minimum time in seconds. This value is compared to the time stamp in the client's request packets, which should represent the time since the client was powered up. Packets are only forwarded when the time stamp exceeds the minimum wait time.
- **Circuit ID Option Mode** — This is the Relay agent option, which can be either Enabled or Disabled. If you select Enable, the relay agent adds Option 82 header packets to the DHCP Request packets before forwarding them to the server, and strips them off while forwarding the responses to the client.
- **Requests Received** — The total number of BOOTP/DHCP requests received from all clients since the last time the switch was reset.
- **Requests Relayed** — The total number of BOOTP/DHCP requests forwarded to the server since the last time the switch was reset.
- **Packets Discarded** — The total number of BOOTP/DHCP packets discarded by this Relay Agent since the last time the switch was reset.

Displaying BOOTP/DHCP using the CLI Command

For information about the CLI command that performs this function, see the following chapter in the *CLI Reference Guide:*

- DHCP and BOOTP Relay Commands

IP Helper

The IP Helper feature allows the switch to forward certain configured UDP broadcast packets to a particular IP address. This allows various applications, such as the DHCP relay agent, to reach servers on non-local subnets, even if the application was designed to assume a server is always on a local subnet and uses broadcast packets (with either the limited broadcast address 255.255.255.255, or a network directed broadcast address) to reach the server.

You can configure relay entries both globally and on specific routing interfaces. Each relay entry maps an ingress interface and destination UDP port number to a single IPv4 address (the helper address). You can configure multiple relay entries for the same interface and UDP port, in which case the relay agent relays matching packets to each server address. Interface configuration takes priority over global configuration. In other words, if the destination UDP port of a packet matches any entry on the ingress interface, the packet is handled according to the interface configuration. If the packet does not match any entry on the ingress interface, the packet is handled according to the global IP helper configuration.

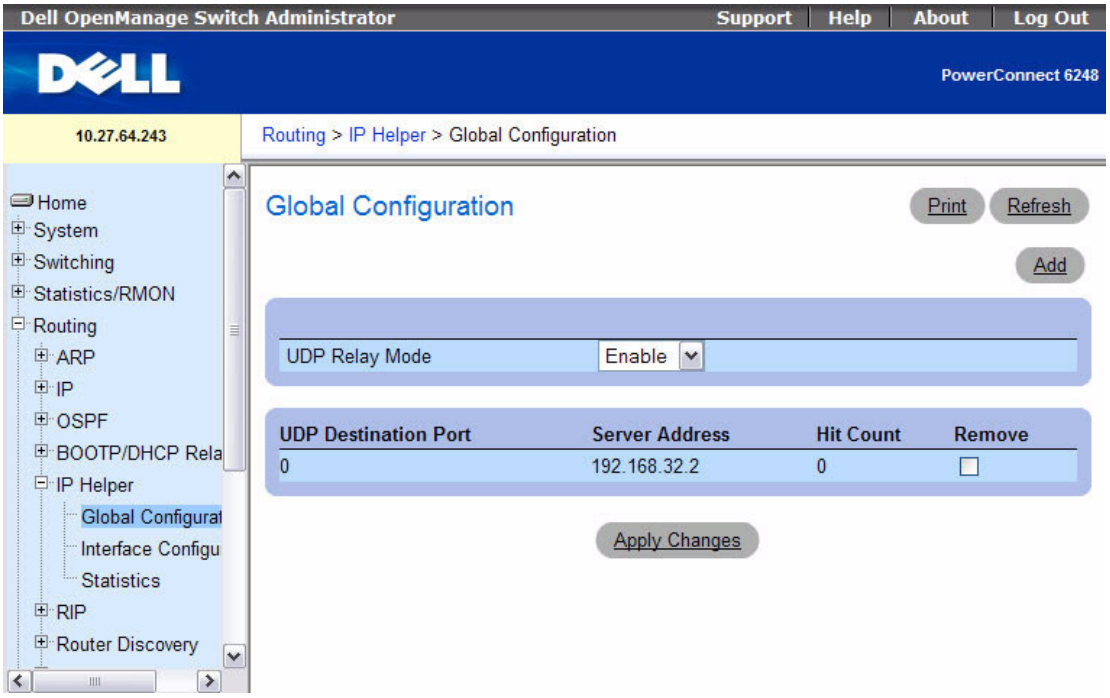
Downloaded from www.Manualslib.com manuals search engine

IP Helper Global Configuration

Use the IP Helper **Global Configuration** page to add, show, or delete UDP Relay and Helper IP configuration

To display the page, click **Routing > IP Helper > Global Configuration** in the tree view.

Figure 9-23. IP Helper Global Configuration



Downloaded from www.Manualslib.com manuals search engine

The IP Helper **Global Configuration** page contains the following fields:

- **UDP Relay Mode** — Use the menu to enable or disable the UDP relay mode. You must enable the UDP Relay Mode to relay any other protocols for which an IP helper address has been configured. By default UDP Relay Mode is Enabled.
- **UDP Destination Port** — Identifies destination UDP port number of UDP packets to be relayed. Table 9-1 lists UDP Port allocations.

Table 9-1. UDP Port Allocations

UDP Port Number	Acronym	Application
7	Echo	Echo
11	SysStat	Active User
15	NetStat	NetStat
17	Quote	Quote of the day
19	CHARGEN	Character Generator
20	FTP-data	FTP Data
21	FTP	FTP
37	Time	Time
42	NAMESERVER	Host Name Server
43	NICNAME	Who is
53	DOMAIN	Domain Name Server
69	TFTP	Trivial File Transfer
111	SUNRPC	Sun Microsystems Rpc
123	NTP	Network Time
137	NetBiosNameService	NT Server to Station Connections
138	NetBiosDatagramService	NT Server to Station Connections
139	NetBios	SessionServiceNT Server to Station Connections
161	SNMP	Simple Network Management
162	SNMP-trap	Simple Network Management Traps
513	who	Unix Rwho Daemon
514	syslog	System Log
525	timed	Time Daemon

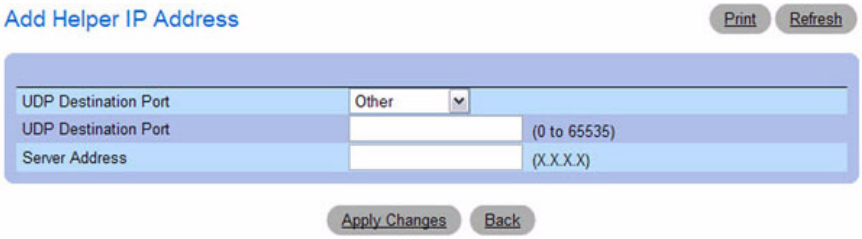
Downloaded from www.Manualslib.com manuals search engine

- **Server Address —** The IPv4 address of the server to which packets are relayed for the specific UDP Destination Port.
- **Hit Count —** The number of times a packet has been forwarded or discarded according to this entry.
- **Remove —** Removes the specified **UDP Relay** when selected and **Apply Changes** is pressed.

Adding an IP Helper Entry

1. Open the IP Helper **Global Configuration** page.
2. Click **Add** to display the **Add Helper IP Address** page:

Figure 9-24. Add Helper IP Address



3. Select a UDP Destination port name from the menu or enter the UDP Destination Port ID. Select the Default Set to configure for the relay entry for the default set of protocols.

   NOTE: If the DefaultSet option is specified, the device by default forwards UDP Broadcast packets for the following services: IEN-116 Name Service (port 42), DNS (port 53), NetBIOS Name Server (port 137), NetBIOS Datagram Server (port 138), TACACS Server (Port 49), and Time Service (port 37).

4. Enter the IP address of the server to which the packets with the given UDP Destination Port will be relayed.
5. Click **Apply Changes**.

   The UDP/Helper Relay is added and the device is updated.

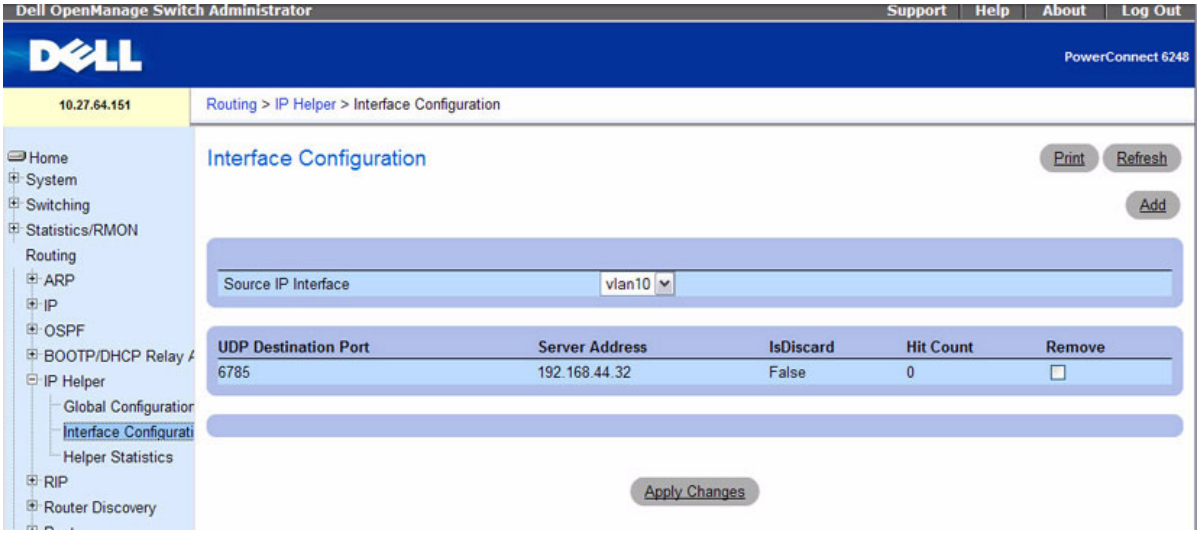
Downloaded from www.Manualslib.com manuals search engine

IP Helper Interface Configuration

Use the IP Helper **Interface Configuration** page to add, show, or delete UDP Relay and Helper IP configuration for a specific interface.

To display the page, click **Routing > IP Helper > Interface Configuration** in the tree view.

Figure 9-25. IP Helper Interface Configuration



The IP Helper **Interface Configuration** page contains the following fields:

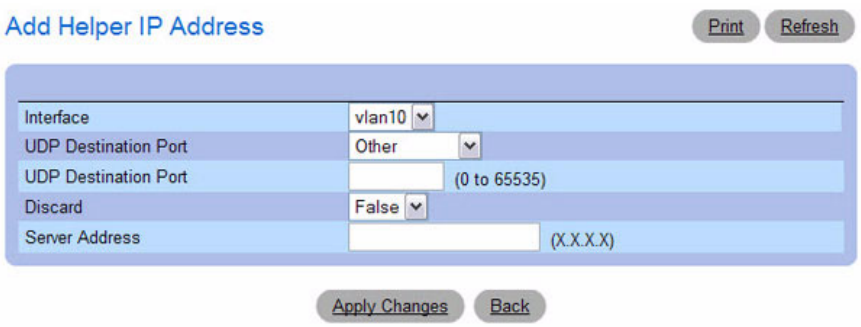
- **Source IP Interface** — Select the interface to use for UDP/Helper relays. Select All to configure relay entries on all available interfaces.
- **UDP Destination Port** — Identifies destination UDP port number of UDP packets to be relayed. For a list of UDP Port allocations, see Table 9-1.
- **Server Address —** The IPv4 address of the server to which packets are relayed for the specific UDP Destination Port.
- **IsDiscard** — If True, packets arriving on the given interface with the given destination UDP port are discarded rather than relayed. Discard entries are used to override global IP helper address entries which otherwise might apply to a packet.
- **Hit Count —** The number of times a packet has been forwarded or discarded according to this entry.
- **Remove** — Select this option and click **Apply Changes** to remove the relay from the selected source IP interface.

Downloaded from www.Manualslib.com manuals search engine

Adding an IP Helper Entry to an Interface

1. Open the IP Helper **Interface Configuration** page.
2. Click **Add** to display the **Interface Configuration Add** page:

Figure 9-26. Add Helper IP Address



3. Select the interface to use for the relay.
4. Select a UDP Destination port name from the menu or enter the UDP Destination Port ID. Select the Default Set to configure for the relay entry for the default set of protocols.

   NOTE: If the DefaultSet option is specified, the device by default forwards UDP Broadcast packets for the following services: IEN-116 Name Service (port 42), DNS (port 53), NetBIOS Name Server (port 137), NetBIOS Datagram Server (port 138), TACACS Server (Port 49), and Time Service (port 37).

5. Choose whether to discard (True) or keep (False) packets arriving on the given interface with the given destination UDP port.
6. Enter the IP address of the server to which the packets with the given UDP Destination Port will be relayed.
7. Click **Apply Changes**.

   The UDP/Helper Relay is added to the interface and the device is updated.

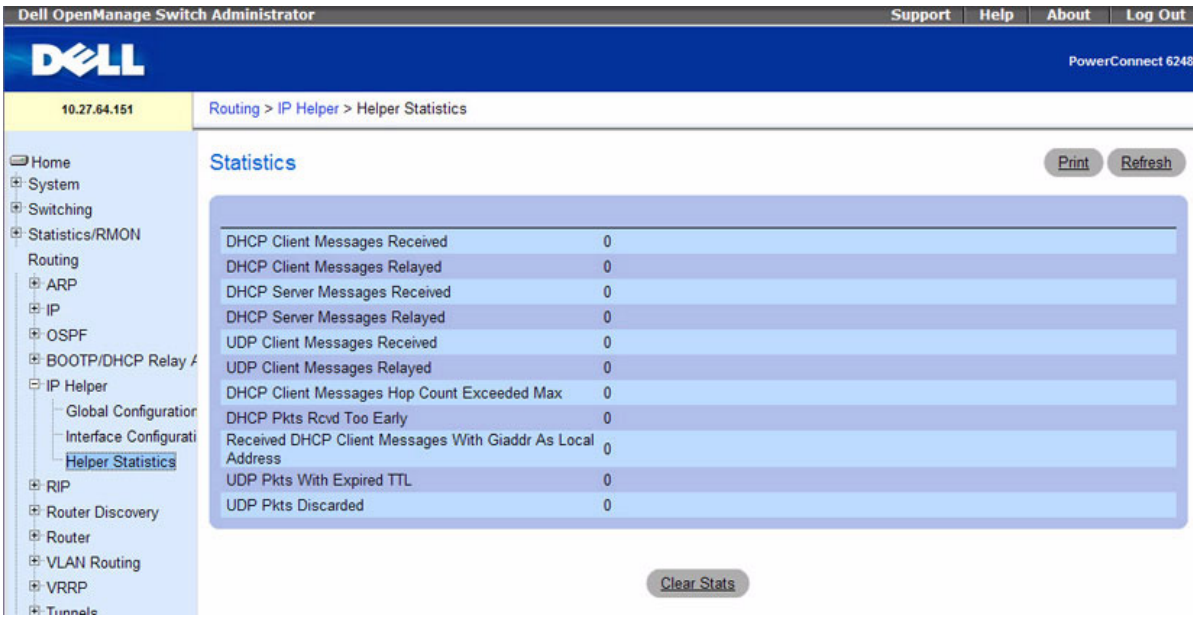
Downloaded from www.Manualslib.com manuals search engine

IP Helper Statistics

Use the IP Helper **Statistics** page to view UDP Relay Statistics for the switch.

To display the page, click **Routing > IP Helper > Statistics** in the tree view.

Figure 9-27. IP Helper Statistics



The IP Helper **Statistics** page contains the following fields:

- **DHCP Client Messages Received** — The number of valid messages received from a DHCP client. The count is only increased if IP helper is enabled globally, the ingress routing interface is up, and the packet passes a number of validity checks, such as having a TTL >1 and having valid source and destination IP addresses.
- **DHCP Client Messages Relayed** — The number of DHCP client messages relayed to a server. If a message is relayed to multiple servers, the count is increased once for each server.
- **DHCP Server Messages Received** — The number of DHCP responses received from the DHCP server. This count only includes messages that the DHCP server unicasts to the relay agent for relay to the client.
- **DHCP Server Messages Relayed** — Specifies the number of DHCP server messages relayed to a client.
- **UDP Client Messages Received** — The number of valid UDP packets received. This count includes DHCP messages and all other protocols relayed. Conditions are similar to those for the first statistic in this table.
- **UDP Client Messages Relayed** — The number of UDP packets relayed. This count includes DHCP messages relayed as well as all other protocols. The count is increased for each server to which a packet is sent.

Downloaded from www.Manualslib.com manuals search engine

- **DHCP Client Messages Hop Count Exceeded Max** — The number of DHCP client messages received whose hop count is larger than the maximum allowed. The maximum hop count is a configurable value.A log message is written for each such failure. The DHCP relay agent does not relay these packets.
- **DHCP Pkts Rcvd Too Early** — The number of DHCP client messages received whose secs field is less than the minimum value. The minimum secs value is a configurable value. A log message is written for each such failure. The DHCP relay agent does not relay these packets.
- **Received DHCP Client Messages With Giaddr As Local Address** — The number of DHCP client messages received whose gateway address, giaddr, is already set to an IP address configured on one of the relay agents own IP addresses. In this case, another device is attempting to spoof the relay agents address. The relay agent does not relay such packets. A log message gives details for each occurrence.
- **UDP Pkts With Expired TTL** — The number of packets received with TTL of 0 or 1 that might otherwise have been relayed.
- **UDP Pkts Discarded** — The number of packets ignored by the relay agent because they match a discard relay entry.

RIP

Routing Information Protocol (RIP) is an Interior Gateway Protocol (IGP) based on the Bellman-Ford algorithm and targeted at smaller networks (network diameter no greater than 15 hops). The routing information is propagated in RIP update packets that are sent out both periodically and in the event of a network topology change. On receipt of a RIP update, depending on whether the specified route exists or does not exist in the route table, the router may modify, delete or add the route to its route table. Route preferences are conveyed through a configurable metric that indicates the distance for each destination.

The **RIP** menu page contains links to web pages that configure and display RIP parameters and data. To display this page, click **Routing > RIP** in the tree view. Following are the web pages accessible from this menu page:

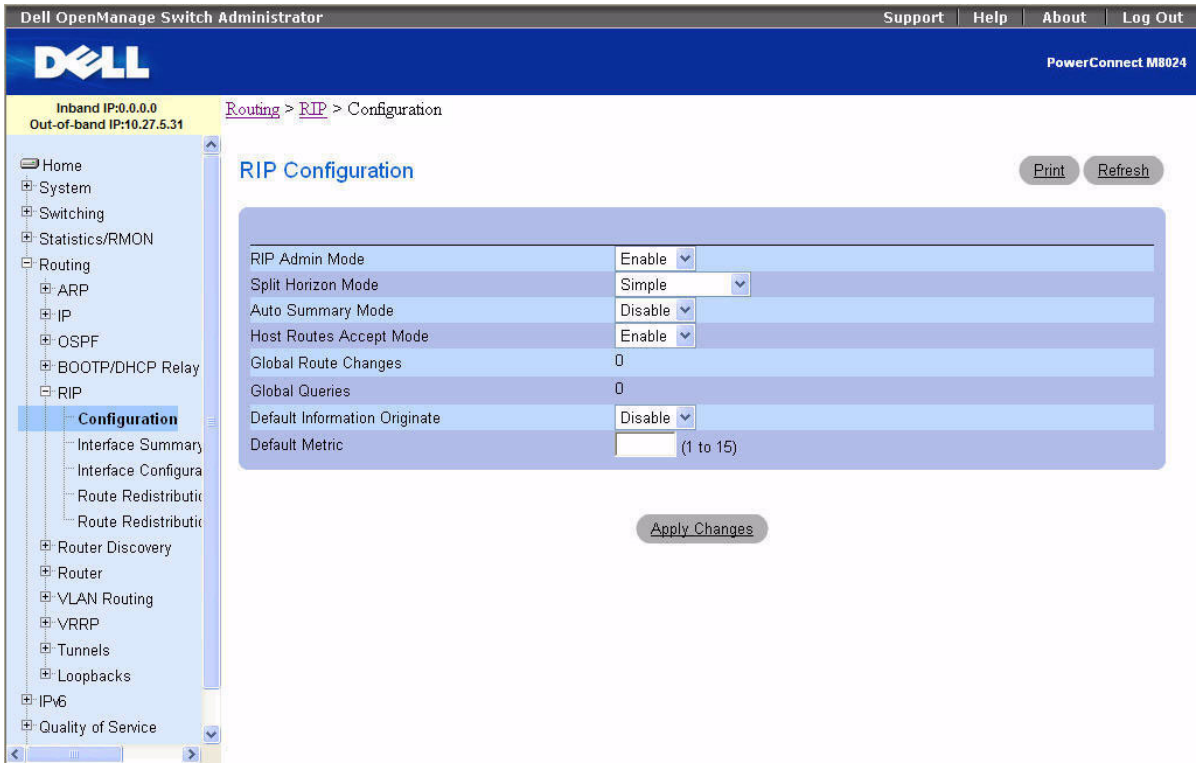
- RIP Configuration
- RIP Interface Summary
- RIP Interface Configuration
- RIP Route Redistribution Configuration
- RIP Route Redistribution Summary

Downloaded from www.Manualslib.com manuals search engine

RIP Configuration

Use the **RIP Configuration** page to enable and configure or disable RIP in Global mode. To display the page, click **Routing > RIP > Configuration** in the tree view.

Figure 9-28. RIP Configuration



The **RIP Configuration** page contains the following fields:

- **RIP Admin Mode** — Select Enable or Disable from the drop-down menu. If you select Enable, RIP is enabled for the switch. The default is Disable.
- **Split Horizon Mode** — Select None, Simple, or Poison Reverse from the drop-down menu. The default is Simple. Split horizon is a technique for avoiding problems caused by including routes in updates sent to the router from which the route was originally learned. The options are:
  - **None** — No special processing for this case.
  - **Simple** — A route is not included in updates sent to the router from which it was learned.
  - **Poison Reverse** — A route is included in updates sent to the router from which it was learned, but the metric is set to infinity.
- **Auto Summary Mode** — Select Enable or Disable from the drop-down menu. If you select Enable, groups of adjacent routes are summarized into single entries, in order to reduce the total number of entries. The default is Enable.

Downloaded from www.Manualslib.com manuals search engine

- **Host Routes Accept Mode** — Select Enable or Disable from the drop-down menu. If you select Enable, the router accepts host routes. The default is Enable.
- **Global Route Changes** — Displays the number of route changes made to the IP Route Database by RIP. This does not include the refresh of a route's age.
- **Global Queries** — Displays the number of responses sent to RIP queries from other systems.
- **Default Information Originate** — Enable or Disable Default Route Advertise.
- **Default Metric** — Sets a default for the metric of redistributed routes.This field displays the default metric if one has already been set, or blank if not configured earlier. Valid values are 1 to 15.

Configuring RIP

1. Open the **RIP Configuration** page.
2. Enter data in the fields as needed.
3. Click **Apply Changes** when finished.

   RIP is configured, and the device is updated.

Configuring RIP using the CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide:*

- Routing Information Protocol (RIP) Commands

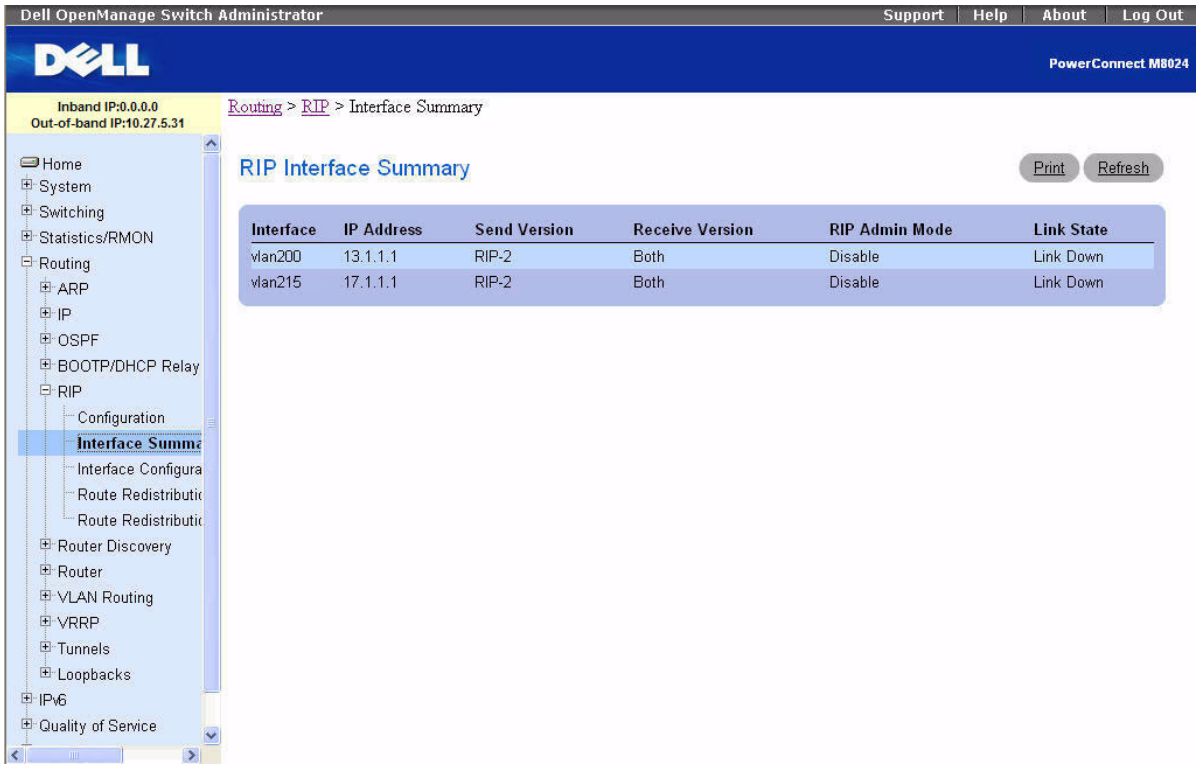
Downloaded from www.Manualslib.com manuals search engine

RIP Interface Summary

Use the **RIP Interface Summary** page to display RIP configuration status on an interface.

To display the page, click **Routing > RIP > Interface Summary** in the tree view.

Figure 9-29. RIP Interface Summary



The **RIP Interface Summary** page displays the following fields:

- **Interface** — The interface, such as the routing-enabled VLAN on which RIP is enabled.
- **IP Address** — The IP Address of the router interface.
- **Send Version** — Specifies the RIP version to which RIP control packets sent from the interface conform. The default is RIP-2. Possible values are:
  - **RIP-1** — RIP version 1 packets are sent using broadcast.
  - **RIP-1c** — RIP version 1 compatibility mode. RIP version 2 formatted packets are transmitted using broadcast.
  - **RIP-2** — RIP version 2 packets are sent using multicast.
  - **None** — RIP control packets are not transmitted.

Downloaded from www.Manualslib.com manuals search engine

- **Receive Version** — Specifies which RIP version control packets are accepted by the interface. The default is Both. Possible values are:
  - **RIP-1** — only RIP version 1 formatted packets are received.
  - **RIP-2** — only RIP version 2 formatted packets are received.
  - **Both** — packets are received in either format.
  - **None** — no RIP control packets are received.
- **RIP Admin Mode** — Specifies whether RIP is Enabled or Disabled on the interface.
- **Link State** — Specifies whether the RIP interface is up or down.

Displaying RIP Interface Summary using the CLI Command

For information about the CLI command that performs this function, see the following chapter in the *CLI Reference Guide:*

- Routing Information Protocol (RIP) Commands

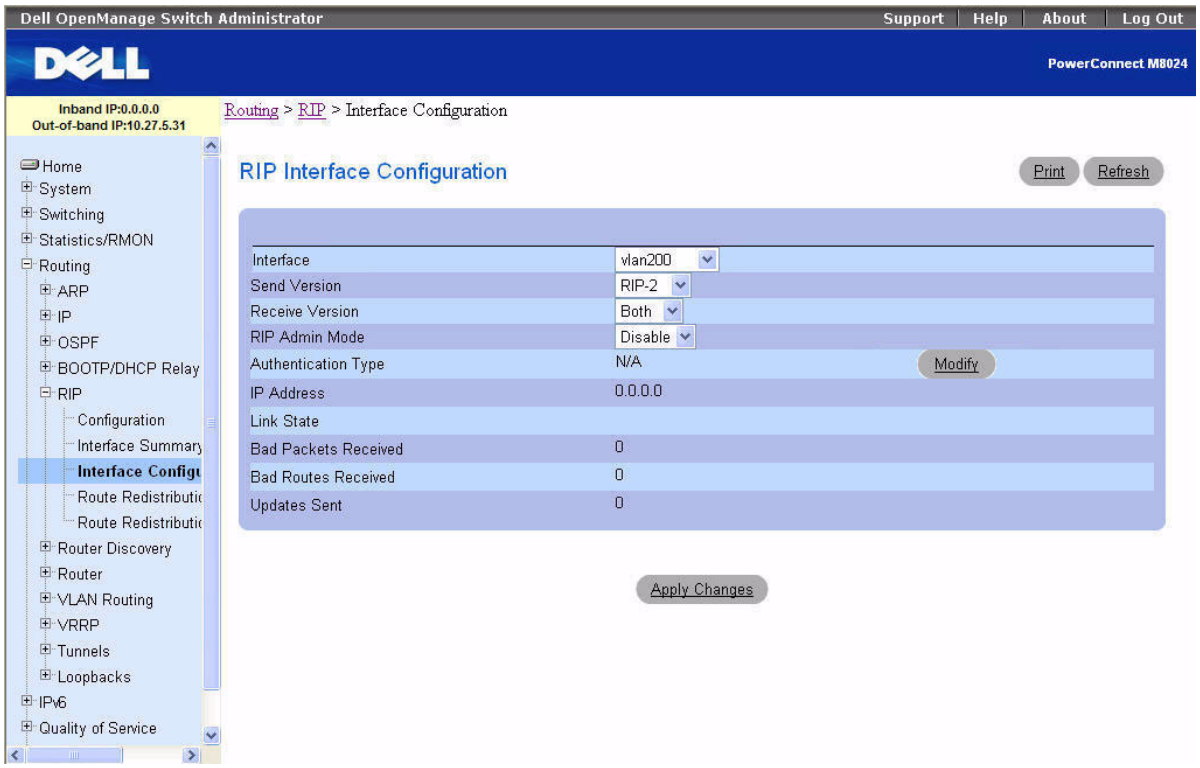
Downloaded from www.Manualslib.com manuals search engine

RIP Interface Configuration

Use the **RIP Interface Configuration** page to enable and configure or to disable RIP on a specific interface.

To display the page, click **Routing > RIP > Interface Configuration** in the tree view.

Figure 9-30. RIP Interface Configuration



The **RIP Interface Configuration** page contains the following fields:

- **Interface** — Select the interface for which data is to be configured from the drop-down menu.
- **Send Version** — RIP Version that router sends with its routing updates. The default is RIP-2. Possible values are:
  - **RIP-1** — send RIP version 1 formatted packets through broadcast.
  - **RIP-1c** — RIP version 1 compatibility mode. Send RIP version 2 formatted packets through broadcast.
  - **RIP-2** — send RIP version 2 packets using multicast.
  - **None** — no RIP control packets are sent.
- **Receive Version** — RIP Version of the routing updates that the router must accept. The default is Both. Possible values are:
  - **RIP-1** — accept only RIP version 1 formatted packets.

Downloaded from www.Manualslib.com manuals search engine

- **RIP-2** — accept only RIP version 2 formatted packets.
- **Both** — accept packets in either format.

- **None** — no RIP control packets is accepted.
- **RIP Admin Mode** — Select Enable or Disable from the drop-down menu. Before you enable RIP version 1 or version 1c on an interface, you must first enable network directed broadcast mode on the corresponding interface. The default value is Disable.
- **Authentication Type** — You may select an authentication type other than None by clicking the **Modify** button. You then see a new screen, where you can select the authentication type from the drop-down menu. Possible values are:
  - **None** — This is the initial interface state. If you select this option from the drop-down menu on the second screen and click **Apply Changes**, you are returned to the first screen without any authentication protocols being run.
  - **Simple** — If you select Simple you are prompted to enter an authentication key. This key is included, in the clear, in the RIP header of all packets sent on the network. All routers on the network must be configured with the same key.
  - **Encrypt** — If you select Encrypt you are prompted to enter both an authentication key and an authentication ID. Encryption uses the MD5 Message-Digest algorithm. All routers on the network must be configured with the same key and ID.
- **IP Address** — Displays the IP Address of the router interface.
- **Link State** — Specifies whether the RIP interface is up or down.
- **Bad Packets Received** — Displays the number of RIP packets that were found to be invalid or corrupt. This explicitly does NOT include full updates sent containing new information.
- **Bad Routes Received** — Displays the number of routes, in valid RIP packets, which were ignored for any reason, for example, the number of triggered RIP updates actually sent on this interface. This explicitly does NOT include full updates sent containing new information.
- **Updates Sent** — Displays the number of Route updates sent.

Downloaded from www.Manualslib.com manuals search engine

Configuring the RIP Interface

1. Open the **RIP Interface Configuration** page.
2. Specify the interface for which data is to be configured.
3. Enter data into the fields as needed:

   Send Version — From the drop-down box, select **None**, **RIP-1**, **RIP-1c**, or **RIP2**.

   Receive Version — From the drop-down box select **None**, **RIP-1**, **RIP-2**, or **Both.**

   RIP Admin Mode — Select **Enable** or **Disable**.

   Authentication Type — Click the **Modify** button to configure different Authentication Types.
4. Click **Apply Changes** when finished.

The RIP interface is configured, and the device is updated.

Selecting an Authentication Method

1. Open the **RIP Interface Configuration** page.
2. Specify the interface for which the authentication method is to be configured.
3. Click **Modify**.

   The Authentication Method page displays.
4. Specify the Authentication Type (None, Simple, or Encrypt) from the drop-down menu.
5. If you specify Simple or Encrypt as the Authentication Type, additional fields appear. Enter the Authentication Key (Simple or Encrypt) and Authentication Key ID (Encrypt).
6. Click **Apply Changes**.
7. The authentication method is updated, and the device is updated.

Configuring the RIP Interface with the CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide:*

- Routing Information Protocol (RIP) Commands

RIP Route Redistribution Configuration

Use the **RIP Route Redistribution Configuration** page to configure the RIP Route Redistribution parameters. The allowable values for each fields are displayed next to the field. If any invalid values are entered, an alert message is displayed with the list of all the valid values.

Downloaded from www.Manualslib.com manuals search engine

Static Reject Routes

A static reject route is a static route to discard the packets to a particular destination, thereby forcing a black-hole routing behavior for a particular set of IP prefixes. Static reject routes can help prevent a routing loop in the network if a default route is configured on a router. Static reject routes also help protect against a DOS attack on a router with unwanted destination addresses.

NOTE: Static reject routes are not redistributed by OSPF or RIP.

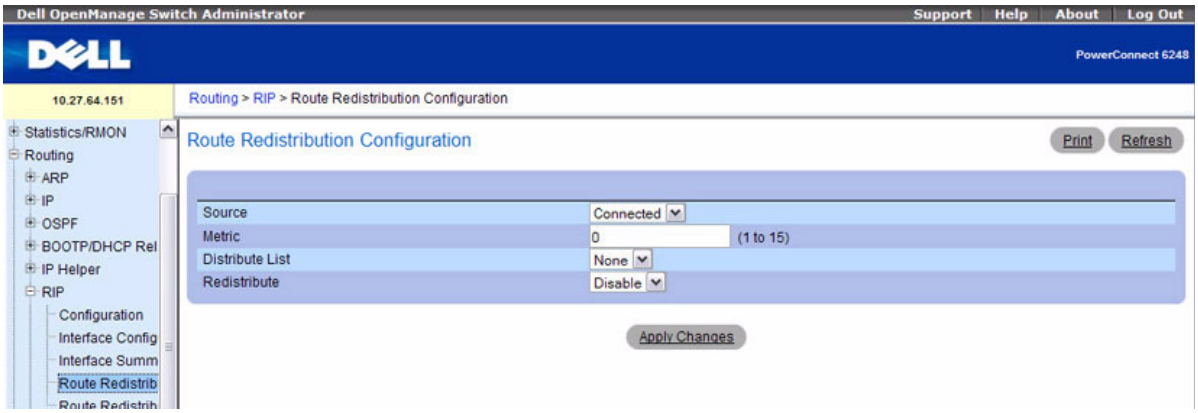
Starting with software release 3.0, you can select Static Reject as a route type from the Route Type field on the following pages under the **Routing > Router** menu:

- Route Entry Configuration
- Configured Routes

NOTE: For a static reject route, the next hop interface value is Null0. Packets to the network address specified in static reject routes are intentionally dropped.

To display the page, click **Routing > RIP > Route Redistribution Configuration** in the tree view.

Figure 9-31. RIP Route Redistribution Configuration



The **RIP Route Redistribution Configuration** page contains the following fields:

- **Source** — Select the type of source route to configure for redistribution by RIP. Possible values are:
  - **Static**
  - **Connected**
  - **OSPF**
- **Metric** — Sets the metric value to be used as the metric of redistributed routes. This field displays the metric if the source was pre-configured and can be modified. The valid values are 1 to 15.
- **Distribute List** — Select the Access List that filters the routes to be redistributed by the destination protocol. Only permitted routes are redistributed.

Downloaded from www.Manualslib.com manuals search engine

The drop-down menu lists the ACLs configured through the pages under **Switching→Network Security→Access Control Lists→IP Access Control Lists**. When used for route filtering, the only fields in an access list that get used are:

– Source IP Address and netmask

– Destination IP Address and netmask

– Action (Permit or Deny)

All other fields (source and destination port, precedence, tos, etc.) are ignored.

The source IP address is compared to the destination IP address of the route. The source IP netmask in the access list rule is treated as a wildcard mask, indicating which bits in the source IP address must match the destination address of the route.

NOTE: A 1 in the mask indicates a Don't Care in the corresponding address bit.

When an access list rule includes a destination IP address and netmask (an extended access list), the destination IP address is compared to the network mask of the destination of the route. The destination netmask in the access list serves as a wildcard mask, indicating which bits in the route's destination mask are significant for the filtering operation.

- **Redistribute** — Enables or disables the redistribution for the selected source protocol. This field has to be enabled in order to be able to configure any of the route redistribution attributes.

Creating a Configured Source

1. Open the **RIP Route Redistribution Configuration** page.
2. Select an Available Source to configure.
3. Specify values for the remaining fields.
4. Click **Apply Changes**.

   The specified Source is now configured, and the device is updated.

Modifying a Configured Source

1. Open the **RIP Route Redistribution Configuration** page.
2. Select the Configured Source to modify.
3. Change values on this screen as needed.
4. Click **Apply Changes**

   Specified changes are saved, and the device is updated.

Configuring RIP Route Redistribution using CLI Command

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide:*

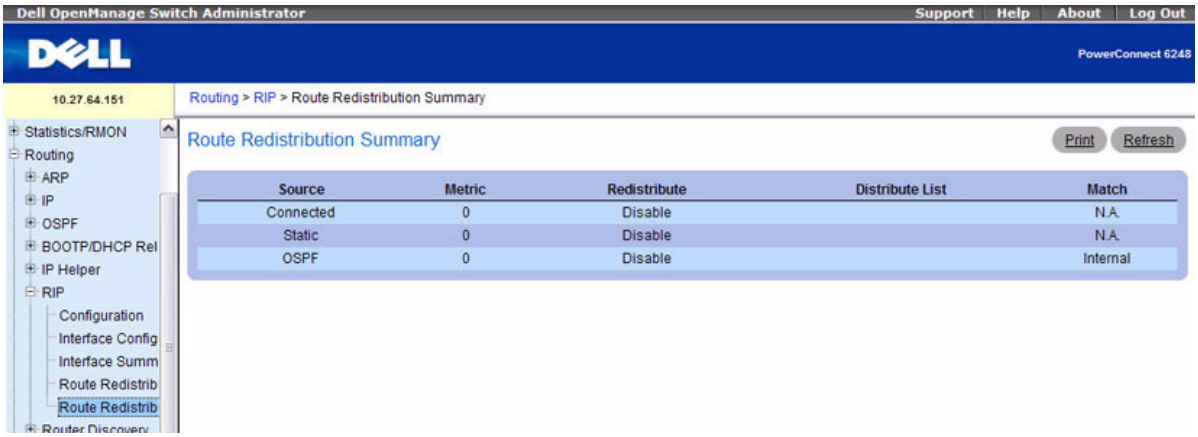
- Routing Information Protocol (RIP) Commands

Downloaded from www.Manualslib.com manuals search engine

RIP Route Redistribution Summary

Use the **RIP Route Redistribution Summary** page to display Route Redistribution configurations. To display the page, click **Routing > RIP > Route Redistribution Summary** in the tree view.

Figure 9-32. RIP Route Redistribution Summary



The **RIP Route Redistribution Summary** page contains the following fields:

- **Source** — The source route to be redistributed by RIP.
- **Metric** — The metric of redistributed routes for the given source route. Displays 0 when not configured.
- Redistribute — Shows whether route redistribution is enabled for the source.
- **Distribute List** — The access list that filters the routes to be redistributed by the destination protocol. If the distribute list is not configured, the field is blank.
- Match — Shows the list of routes redistributed when OSPF is selected as the source, which can be any of the following:
  - **Match Internal** — Shows whether redistribution of OSPF internal routes is enabled.
  - **Match External Type 1** — Shows whether the redistribution of OSPF external type 1 routes is enabled.
  - **Match External Type 2**— Shows whether the redistribution of OSPF external type 2 routes is enabled.
  - **Match NSSA External Type 1** — Shows whether the redistribution of OSPF NSSA external type 1 routes is enabled.
  - **Match NSSA External Type 2**— Shows whether the redistribution of OSPF NSSA external type 2 routes is enabled.

Downloaded from www.Manualslib.com manuals search engine

Displaying RIP Route Redistribution Summary using the CLI Command

For information about the CLI command that performs this function, see the following chapter in the *CLI Reference Guide:*

- Routing Information Protocol (RIP) Commands

Router Discovery

The Router Discovery protocol is used by hosts to identify operational routers on the subnet. Router Discovery messages are of two types: “Router Advertisements” and “Router Solicitations.” The protocol mandates that every router periodically advertise the IP Addresses it is associated with. Hosts listen for these advertisements and discover the IP Addresses of neighboring routers.

The **Router Discovery** menu page contains links to web pages that configure and display Router Discovery data. To display this menu, click **Routing > Router Discovery** in the tree view. Following are the web pages accessible from this menu page:

- Router Discovery Configuration
- Router Discovery Status

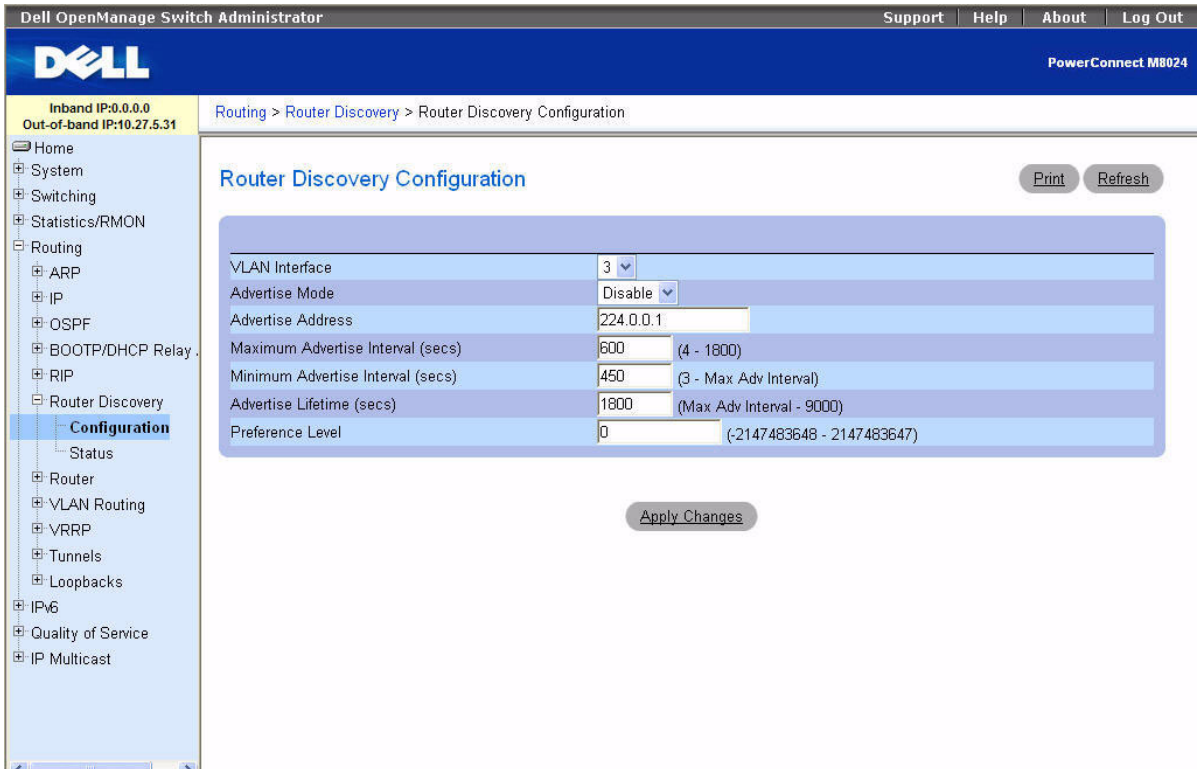
Router Discovery Configuration

Use the **Router Discovery Configuration** page to enter or change Router Discovery parameters.

To display the page, click **Routing > Router Discovery > Configuration** in the tree view.

Downloaded from www.Manualslib.com manuals search engine

Figure 9-33. Router Discovery Configuration



The **Router Discovery Configuration** page contains the following fields:

- **VLAN Interface** — Select the router interface for which data is to be configured.
- **Advertise Mode** — Select Enable or Disable from the drop-down menu. If you select Enable, Router Advertisements are transmitted from the selected interface.
- **Advertise Address** — Enter the IP Address to be used to advertise the router.
- **Maximum Advertise Interval (secs)** — Enter the maximum time (in seconds) allowed between router advertisements sent from the interface.
- **Minimum Advertise Interval (secs)** — Enter the minimum time (in seconds) allowed between router advertisements sent from the interface.
- **Advertise Lifetime (secs)** — Enter the value (in seconds) to be used as the lifetime field in router advertisements sent from the interface. This is the maximum length of time that the advertised addresses are to be considered as valid router addresses by hosts.
- **Preference Level** — Specify the preference level of the router as a default router relative to other routers on the same subnet. Higher numbered addresses are preferred. You must enter an integer.

Downloaded from www.Manualslib.com manuals search engine

Configuring Router Discovery

1. Open the **Router Discovery Configuration** page.
2. Select the router interface to be configured.
3. Configure data as needed for the remaining fields.
4. Click **Apply Changes**

   Specified configuration changes are saved, and the device is updated.

Configuring Router Discovery using the CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide:*

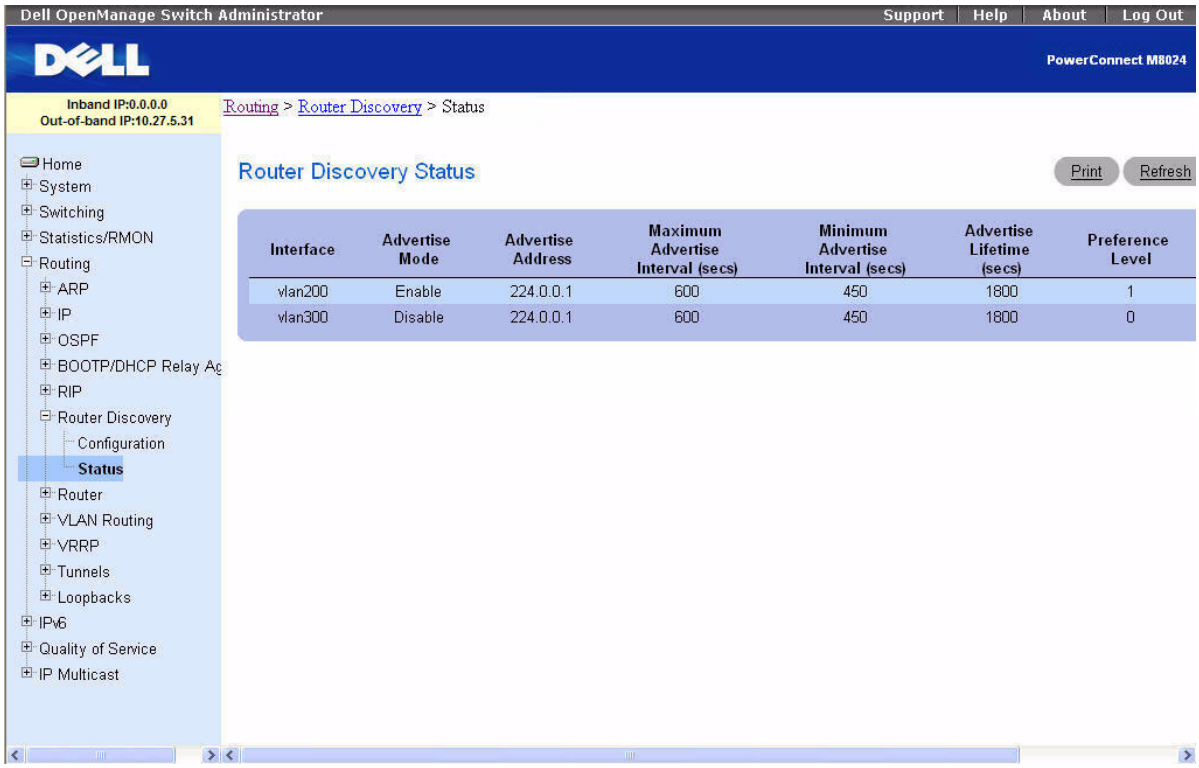
- Router Discovery Protocol Commands

Router Discovery Status

Use the **Router Discovery Status** page to display Router Discovery data for each port.

To display the page, click **Routing > Router Discovery > Status** in the tree view.

Figure 9-34. Router Discovery Status



Downloaded from www.Manualslib.com manuals search engine

The **Router Discovery Status** page displays the following fields:

- **Interface** — The router interface for which data is displayed.
- **Advertise Mode** — The values are Enable or Disable. Enable denotes that Router Discovery is enabled on that interface.
- **Advertise Address** — The IP Address used to advertise the router.
- **Maximum Advertise Interval (secs)** — The maximum time (in seconds) allowed between router advertisements sent from the interface.
- **Minimum Advertise Interval (secs)** — The minimum time (in seconds) allowed between router advertisements sent from the interface.
- **Advertise Lifetime (secs)** — The value (in seconds) used as the lifetime field in router advertisements sent from the interface. This is the maximum length of time that the advertised addresses are to be considered as valid router addresses by hosts.
- **Preference Level** — The preference level of the router as a default router relative to other routers on the same subnet. Higher numbered addresses are preferred.

Displaying Router Discovery Status using the CLI Command

For information about the CLI command that performs this function, see the following chapter in the *CLI Reference Guide:*

- Router Discovery Protocol Commands

Router

The **Router** menu page contains links to web pages that configure and display route tables. To display this page, click **Routing > Router** in the tree view. Following are the web pages accessible from this menu page:

- Route Table
- Best Routes Table
- Route Entry Configuration
- Configured Routes
- Route Preferences Configuration

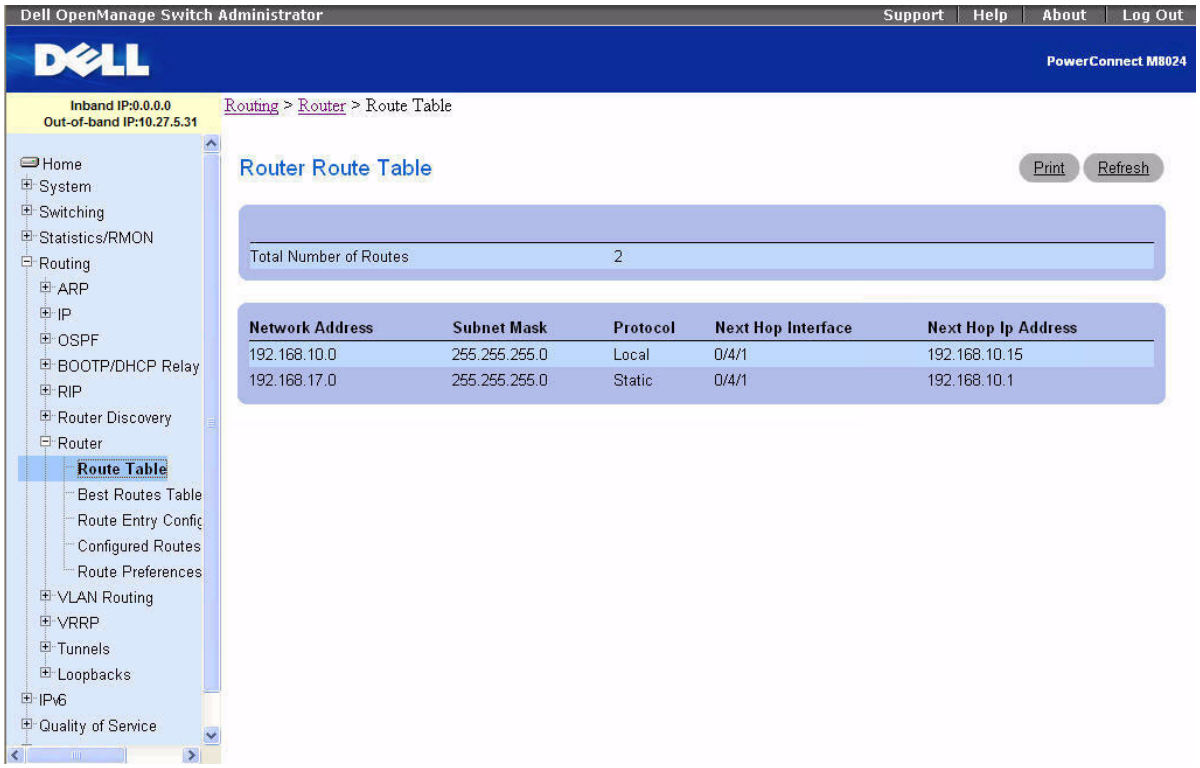
Downloaded from www.Manualslib.com manuals search engine

Route Table

Use the **Router Route Table** page to display the route table configuration.

To display the page, click **Routing > Router > Route Table** in the tree view.

Figure 9-35. Router Route Table



The **Router Route Table** page displays the following fields:

- Total Number of Routes — The total number of routes in the route table.
- **Network Address** — The IP route prefix for the destination.
- **Subnet Mask** — Also referred to as the subnet/network mask, this indicates the portion of the IP interface address that identifies the attached network.
- **Protocol** — This field tells which protocol created the specified route. The possibilities are one of the following:
  - Local
  - Static
  - Default
  - OSPF Intra
  - OSPF Inter

Downloaded from www.Manualslib.com manuals search engine

- OSPF Type-1
- OSPF Type-2
- RIP

- **Next Hop Interface** — The outgoing router interface to use when forwarding traffic to the destination.
- **Next Hop IP Address** — The outgoing router IP address to use when forwarding traffic to the next router (if any) in the path towards the destination. The next router is always one of the adjacent neighbors or the IP address of the local interface for a directly attached network.

Displaying the Router Route Table using the CLI Command

For information about the CLI command that performs this function, see the following chapter in the *CLI Reference Guide:*

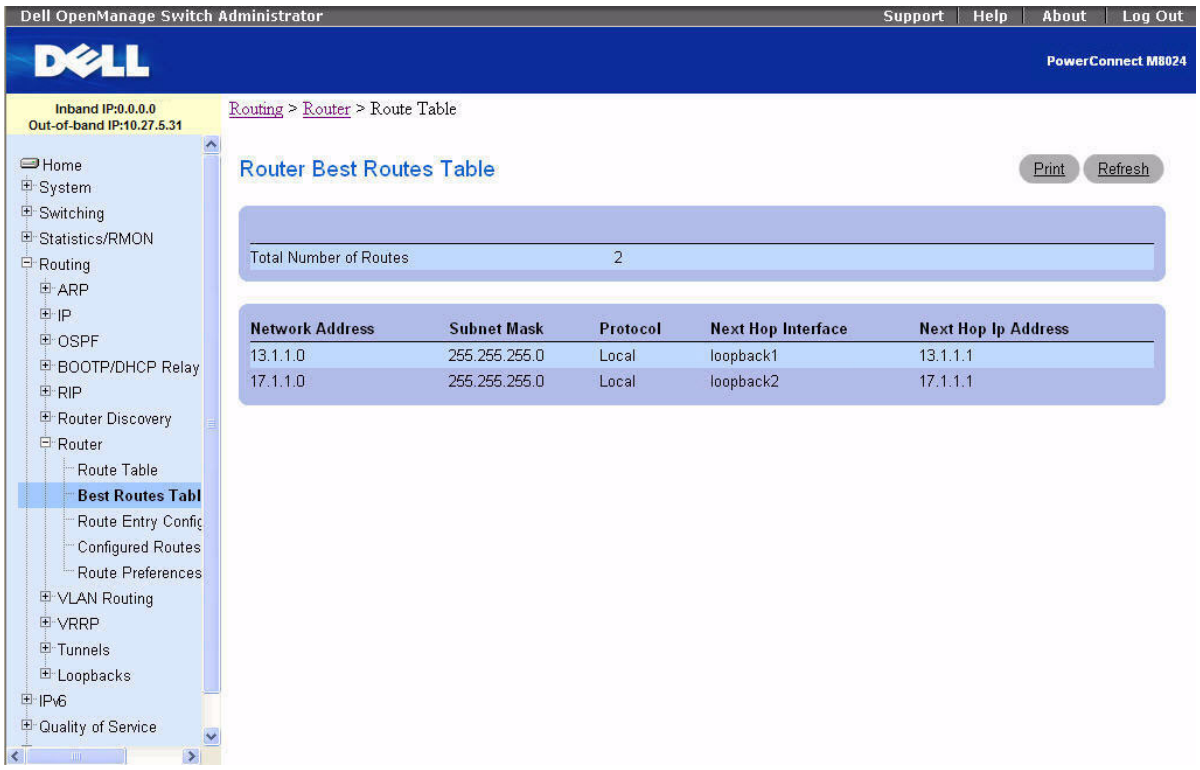
- IP Routing Commands

Best Routes Table

Use the **Router Best Routes Table** page to display the best routes from the routing table.

To display the page, click **Routing > Router > Best Routes Table** in the tree view.

Figure 9-36. Router Best Routes Table



Downloaded from www.Manualslib.com manuals search engine

The **Router Best Routes Table** page displays the following fields:

- **Total Number of Routes** — The total number of routes in the route table.
- **Network Address** — The IP route prefix for the destination.
- **Subnet Mask** — Also referred to as the subnet/network mask, this indicates the portion of the IP interface address that identifies the attached network.
- **Protocol** — This field tells which protocol created the specified route. The possibilities are one of the following:
  - Local
  - Static
  - Default
  - OSPF Intra
  - OSPF Inter
  - OSPF Type-1
  - OSPF Type-2
  - RIP
- **Next Hop Interface** — The outgoing router interface to use when forwarding traffic to the destination.
- **Next Hop IP Address** — The outgoing router IP address to use when forwarding traffic to the next router (if any) in the path towards the destination. The next router is always one of the adjacent neighbors or the IP address of the local interface for a directly attached network.

Displaying the Best Routes Table using the CLI Command

For information about the CLI command that performs this function, see the following chapter in the *CLI Reference Guide:*

- IP Routing Commands

Downloaded from www.Manualslib.com manuals search engine

Route Entry Configuration

Use the **Router Route Entry Configuration** page to add new and configure router routes.

To display the page, click **Routing > Router > Route Entry Configuration** in the tree view.

Figure 9-37. Router Route Entry Configuration

The **Router Route Entry Configuration** page contains the following fields:

- **Network Address** — Specify the IP route prefix for the destination from the drop-down menu. In order to create a route, a valid routing interface must exist and the next hop IP Address must be on the same network as the routing interface. Routing interfaces are created on the **IP Interface Configuration** page. Valid next hop IP Addresses can be viewed on the **Route Table** page.
- **Subnet Mask** — Also referred to as the subnet/network mask, this indicates the portion of the IP interface address that identifies the attached network.
- **Protocol** — This field tells which protocol created the specified route. Possible values are:
  - Local
  - Static
  - Default
  - OSPF Intra
  - OSPF Inter

Downloaded from www.Manualslib.com manuals search engine

- OSPF Type-1
- OSPF Type-2
- RIP

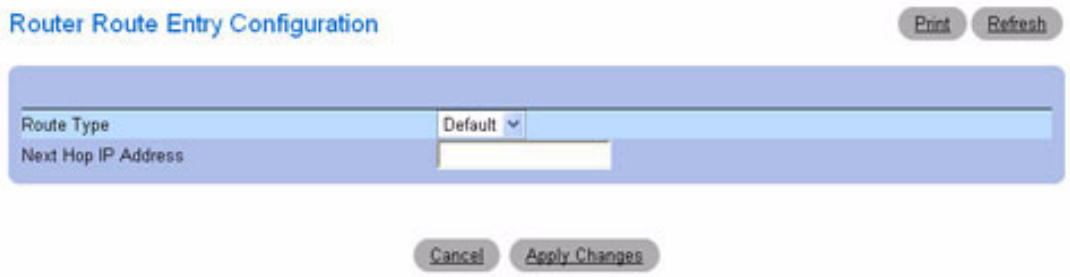
- **Next Hop Interface** — The outgoing router interface to use when forwarding traffic to the destination.
- **Next Hop IP Address** — The outgoing router IP address to use when forwarding traffic to the next router (if any) in the path towards the destination. The next router is always one of the adjacent neighbors or the IP address of the local interface for a directly attached network. When creating a route, the next hop IP must be on the same network as the routing interface. Valid next hop IP Addresses can be seen on the 'Route Table' page.
- **Metric** — Administrative cost of the path to the destination. If no value is entered, default is 1. The range is 0–255.This field is present only when creating a static route.
- **Preference** — Specifies a preference value for the configured next hop.

Adding a Router Route

1. Open the **Router Route Entry Configuration** page.
2. Click **Add Route**.

   The screen refreshes and the **Router Route Entry Configuration** page displays new fields as shown in Figure 9-38.

Figure 9-38. Add Route - Default Route Type



3. Next to **Route Type,** use the drop-down box to add a **Default** route or a **Static** route.

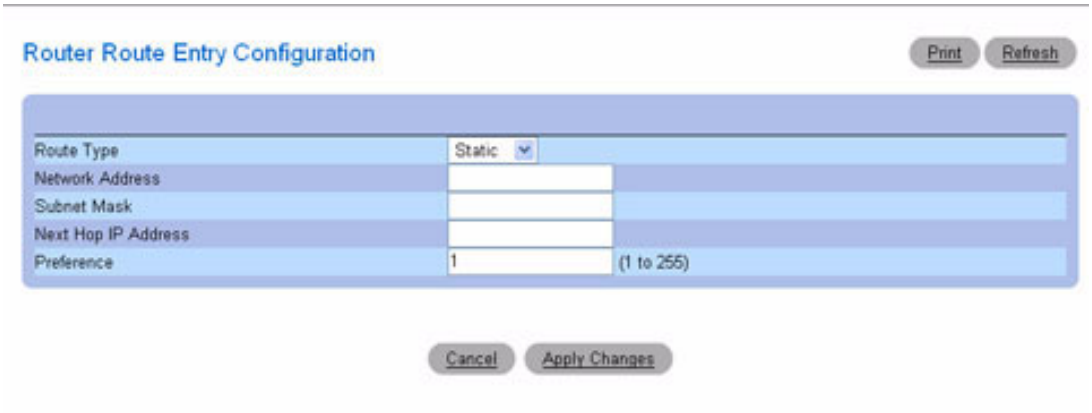
   If you select Static, the page refreshes and new fields appear, as Figure 9-39 shows.

   Default — Enter the default gateway address in the **Next Hop IP Address** field.

   Static — Enter values for **Network Address**, **Subnet Mask**, **Next Hop IP Address**, and **Preference**.

Downloaded from www.Manualslib.com manuals search engine

Figure 9-39. Route Entry Configuration - Add Static Route Type



4. Click **Apply Changes**.

   The new route is added, and you are redirected to the Configured Routes page.

Adding a Router Route using the CLI Command

For information about the CLI command that performs this function, see the following chapter in the *CLI Reference Guide:*

- IP Routing Commands

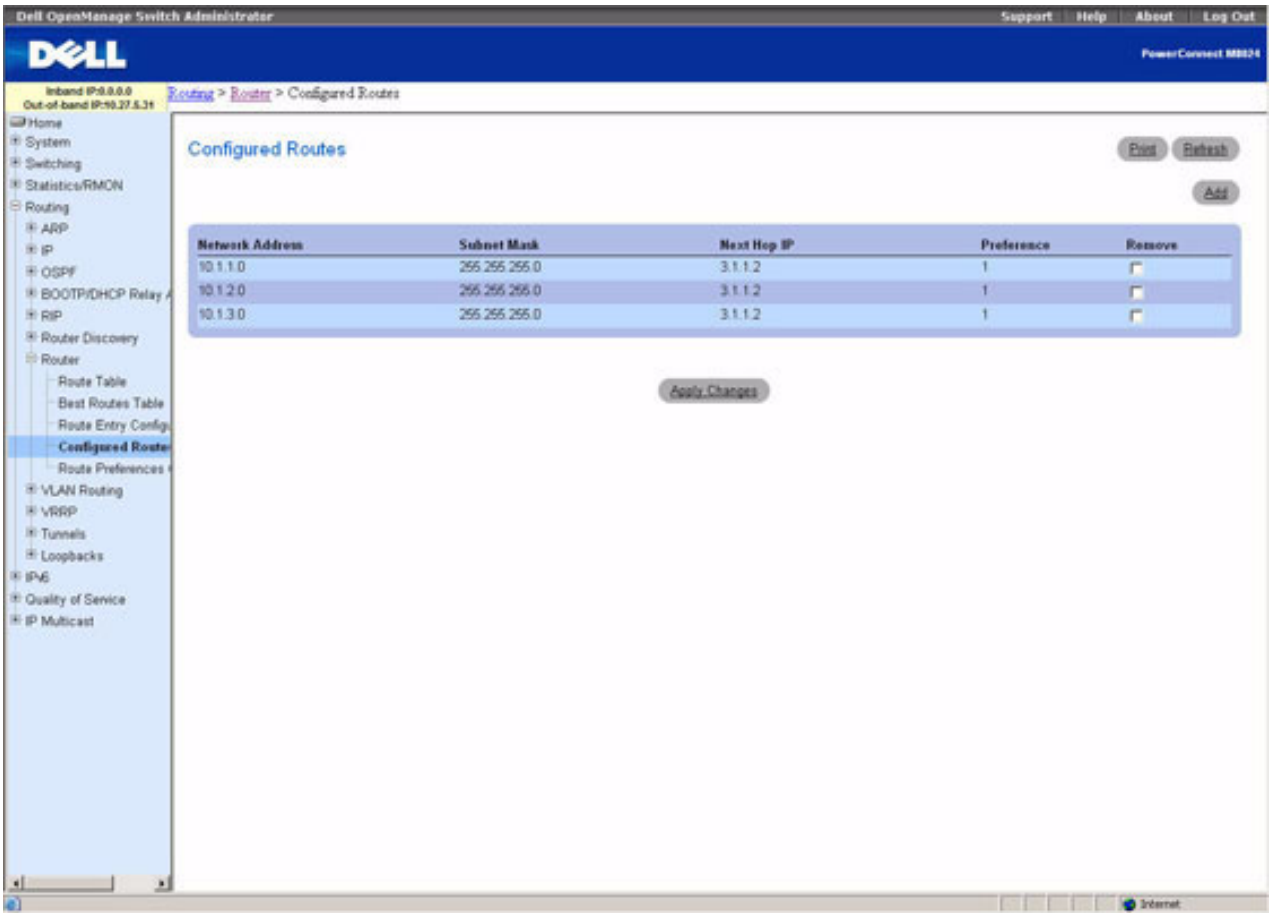
Downloaded from www.Manualslib.com manuals search engine

Configured Routes

Use the **Configured Routes** page to display the routes that have been configured.

To display the page, click **Routing > Router > Configured Routes** in the tree view.

Figure 9-40. Configured Routes



The **Configured Routes** page displays the following fields:

- **Network Address** — The IP route prefix for the destination.
- **Subnet Mask** — Also referred to as the subnet/network mask, this indicates the portion of the IP interface address that identifies the attached network.
- **Next Hop IP** — The outgoing router interface to use when forwarding traffic to the destination.
- **Preference** — Displays the preferences configured for the added routes.
- **Remove** — Use this check box to remove a configured route.

Downloaded from www.Manualslib.com manuals search engine

Adding a Router Route

1. Open the **Configured Routes** page.
2. Click **Add**.

   The **Router Route Entry Configuration** page displays, as Figure 9-38 shows.
3. Next to **Route Type,** use the drop-down box to add a **Default** route or a **Static** route.

   Default — Enter the default gateway address in the **Next Hop IP Address** field. Figure 9-38 shows the fields that display when the **Route Type** value is Default.

   Static — Enter values for **Network Address**, **Subnet Mask**, **Next Hop IP Address**, and **Preference**. Figure 9-39 shows the fields that display when the **Route Type** value is Static.
4. Click **Apply Changes**.

   The new route is added, and you are returned to the Configured Routes page.

Displaying Configured Routes using the CLI Command

For information about the CLI command that performs this function, see the following chapter in the *CLI Reference Guide:*

- IP Routing Commands

Route Preferences Configuration

Use the **Router Route Preferences Configuration** page to configure the default preference for each protocol (for example 60 for static routes). These values are arbitrary values that range from 1 to 255, and are independent of route metrics. Most routing protocols use a route metric to determine the shortest path known to the protocol, independent of any other protocol.

The best route to a destination is chosen by selecting the route with the lowest preference value. When there are multiple routes to a destination, the preference values are used to determine the preferred route. If there is still a tie, the route with the best route metric is chosen. To avoid problems with mismatched metrics (i.e. RIP and OSPF metrics are not directly comparable), you must configure different preference values for each of the protocols.

Static Reject Routes

A static reject route is a static route to discard the packets to a particular destination, thereby forcing a black-hole routing behavior for a particular set of IP prefixes. Static reject routes can help prevent a routing loop in the network if a default route is configured on a router. Static reject routes also help protect against a DOS attack on a router with unwanted destination addresses.

NOTE: Static reject routes are not redistributed by OSPF or RIP.

Downloaded from www.Manualslib.com manuals search engine

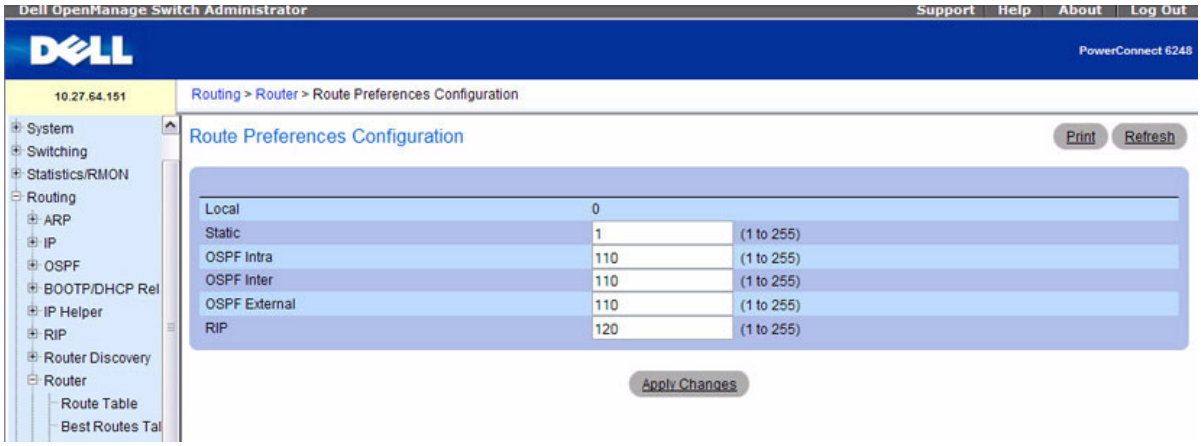
You can select Static Reject as a route type from the Route Type field on the following pages under the **Routing > Router** menu:

- Route Entry Configuration
- Configured Routes

NOTE: For a static reject route, the next hop interface value is Null0. Packets to the network address specified in static reject routes are intentionally dropped.

To display the page, click **Routing > Router > Route Preferences Configuration** in the tree view.

Figure 9-41. Router Route Preferences Configuration



The **Router Route Preferences Configuration** page contains the following fields:

- **Local** — This field displays the local route preference value.
- **Static** — The static route preference value in the router. The default value is 1. The range is 1 to 255.
- **OSPF Intra** — The OSPF intra route preference value in the router. The default value is 110.
- **OSPF Inter** — The OSPF inter route preference value in the router. The default value is 110.
- **OSPF External** — The OSPF External route preference value in the router (OSPF External are OSPF Type-1 and OSPF Type-2 routes). The default value is 110.
- **RIP** — The RIP route preference value in the router. The default value is 120.

Configuring Route Preferences

1. Open the **Route Preferences Configuration** page.
2. Define the applicable fields on this page
3. Click **Apply Changes**.

   The route preferences are configured, and the device is updated.

Downloaded from www.Manualslib.com manuals search engine

Configuring Route Preferences using CLI Command

For information about the CLI command that performs this function, see the following chapter in the *CLI Reference Guide:*

- OSPF Commands

VLAN Routing

You can configure PowerConnect M6220/M6348/M8024 software with some VLANs that support routing. You can also configure the software to allow traffic on a VLAN to be treated as if the VLAN were a router port.

When a port is enabled for bridging (default) rather than routing, all normal bridge processing is performed for an inbound packet, which is then associated with a VLAN. Its MAC Destination Address (MAC DA) and VLAN ID are used to search the MAC address table. If routing is enabled for the VLAN, and the MAC DA of an inbound unicast packet is that of the internal bridge-router interface, the packet is routed. An inbound multicast packet is forwarded to all ports in the VLAN, plus the internal bridge-router interface, if it was received on a routed VLAN.

Since a port can be configured to belong to more than one VLAN, VLAN routing might be enabled for all of the VLANs on the port or for only some of the VLANs on the port. VLAN Routing can be used to allow more than one physical port to reside on the same subnet. It could also be used when a VLAN spans multiple physical networks, or when additional segmentation or security is required. This section shows how to configure the PowerConnect M6220/M6348/M8024 software to support VLAN routing. A port can be either a VLAN port or a router port, but not both. However, a VLAN port may be part of a VLAN that is itself a router port.

The **VLAN Routing** menu page contains a link to a web page that displays VLAN Routing parameters and data. To display this page, click **Routing > VLAN Routing** in the tree view. The following web page is accessible from this menu page:

- VLAN Routing Configuration
- VLAN Routing Summary

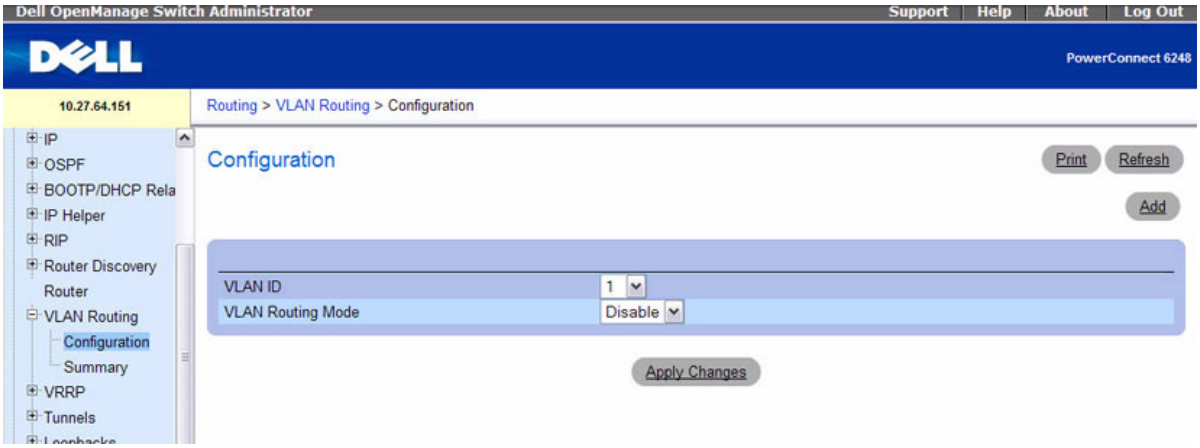
Downloaded from www.Manualslib.com manuals search engine

VLAN Routing Configuration

Use the **VLAN Routing Configuration** page to enable routing on VLAN interfaces and to add VLAN routing interfaces.

To display the page, click **Routing > VLAN Routing > Configuration** in the tree view.

Figure 9-42. VLAN Routing Configuration



The **VLAN Routing Configuration** page displays the following fields:

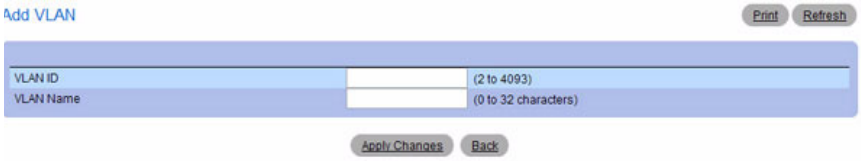
- **VLAN ID** — The ID of the VLAN whose data is displayed in the current table row.
- **VLAN Routing Mode** — Enable or disable routing on the VLAN selected in the VLAN ID field.

Adding New VLANs

1. Open the **VLAN Routing Configuration** page.
2. Click **Add**.

   The **Add VLAN** page displays.

Figure 9-43. Add VLAN



3. Enter a new VLAN ID and VLAN Name.
4. Click **Apply Changes**.

   The new VLAN is added, and the device is updated.

NOTE: To remove a VLAN, use the **Switching→VLAN→VLAN Membership** page.

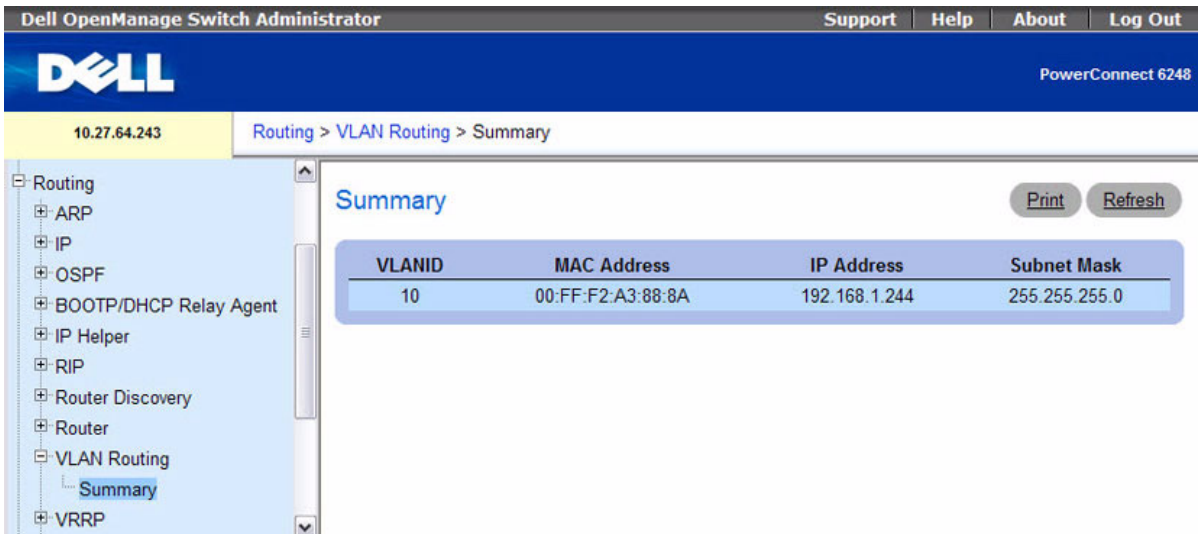
Downloaded from www.Manualslib.com manuals search engine

VLAN Routing Summary

Use the **VLAN Routing Summary** page to display the VLAN routing summary.

To display the page, click **Routing > VLAN Routing > Summary** in the tree view.

Figure 9-44. VLAN Routing Summary



The **VLAN Routing Summary** page displays the following fields:

- **VLAN ID** — The ID of the VLAN whose data is displayed in the current table row.
- **MAC Address** — The MAC Address assigned to the VLAN Routing Interface.
- **IP Address** — The configured IP address of the VLAN Routing Interface.

NOTE: If a VLAN is created and the IP address is not configured, the web page by default shows an IP address of 0.0.0.0. To configure the IP address, go to the **Routing→IP →Interface Configuration** page. See "IP Interface Configuration" on page 461.

- **Subnet Mask** — The configured subnet mask of the VLAN Routing Interface. This is 0.0.0.0 when the VLAN Routing Interface is first configured and must be entered on the **Routing→IP →Interface Configuration** page.

Displaying the VLAN Routing Summary using the CLI Command

For information about the CLI commands that perform this function, see the following chapters in the *CLI Reference Guide:*

- IP Addressing Commands
- Virtual LAN Routing Commands

Downloaded from www.Manualslib.com manuals search engine

VRRP

The Virtual Router Redundancy (VRRP) protocol is designed to handle default router failures by providing a scheme to dynamically elect a backup router. The driving force was to minimize “black hole” periods due to the failure of the default gateway router during which all traffic directed towards it is lost until the failure is detected. Though static configuration of default routes is popular, such an approach is susceptible to a single point of failure when the default router fails. VRRP advocates the concept of a “virtual router” associated with one or more IP Addresses that serve as default gateways. In the event that the VRRP Router controlling these IP Addresses (formally known as the Master) fails, the group of IP Addresses and the default forwarding role is taken over by a Backup VRRP Router.

The VRRP Router Configuration feature enables interface and route tracking. Use VRRP tracking to ensure the best VRRP router is Master for the group.

VRRP interface tracking monitors a specific interface IP state within the router. Depending on the state of the tracked interface, the feature can alter the VRRP priority level of a virtual router for a VRRP group. An exception to the priority level change is that if the VRRP group is the IP address owner, its priority is fixed at 255 and cannot be reduced through the tracking process.

VRRP route tracking monitors the reachability of an IP route. A tracked route is considered up when a routing table entry exists for the route and the route is accessible. To configure route tracking, make VRRP a best route client of RTO. When a tracked route is added or deleted, change the priority.

The **VRRP** menu page contains links to web pages that configure and display parameters and data. To display this page, click **Routing > VRRP** in the tree view. Following are the web pages accessible from this menu page:

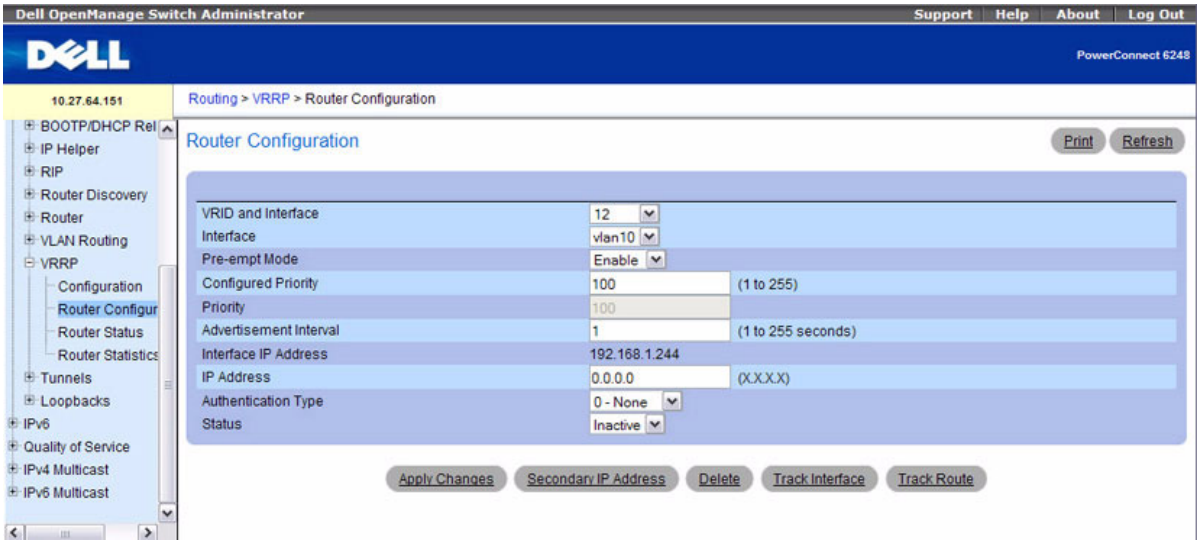
- VRRP Router Configuration
- VRRP Virtual Router Status
- VRRP Virtual Router Statistics

Downloaded from www.Manualslib.com manuals search engine

VRRP Router Configuration

Use the **VRRP Configuration** page to enable or disable the administrative status of a virtual router. To display the page, click **Routing > VRRP > Router Configuration** in the tree view.

Figure 9-45. VRRP Router Configuration



The **Virtual Router Configuration** page contains the following fields:

- **VRID and Interface** — Select **Create** from the drop-down menu to configure a new Virtual Router, or select one of the existing Virtual Routers, listed by interface number and VRID.
- **VRID** — This field is only configurable if you are creating new Virtual Router, in which case enter the VRID in the range 1 to 255.
- **Interface** — This field is only configurable if you are creating new Virtual Router, in which case select the interface for the new Virtual Router from the drop-down menu.
- **Pre-empt Mode** — Select Enable or Disable from the drop-down menu. If you select Enable, a backup router preempts the master router if it has a priority greater than the master virtual router's priority provided the master is not the owner of the virtual router IP address. The default is Enable.
- **Configured Priority** — Enter the priority value to be used by the VRRP router in the election for the master virtual router. If the Virtual IP Address is the same as the interface IP Address, the priority gets set to 255 no matter what you enter. If you enter a priority of 255 when the Virtual and interface IP Addresses are not the same, the priority gets set to the default value of 100.
- **Priority** — The operational priority of the VRRP router, which is relative to the configured priority and depends on the priority decrements configured through tracking process. The priority and configured priority are the same unless a tracked event (for example a tracked interface is down) has occurred to change the value.

Downloaded from www.Manualslib.com manuals search engine

- **Advertisement Interval** — Enter the time, in seconds, between the transmission of advertisement packets by this virtual router. Enter a number between 1 and 255. The default value is 1 second.
- **Interface IP Address** — Indicates the IP Address associated with the selected interface.
- **IP Address** — Enter the IP Address associated with the Virtual Router. The default is 0.0.0.0, which you must change prior to pressing **Create**.
- **Authentication Type** — Select the type of Authentication for the Virtual Router from the drop-down menu. The default is None. The choices are:
  - **0-None** — No authentication is performed.
  - **1-Simple** — Authentication is performed using a text password.
- **Authentication Data** — If you selected simple authentication, enter the password.
- **Status** — Select active or inactive from the drop-down menu to start or stop the operation of the Virtual Router. The default is inactive.

Creating a new Virtual Router

1. Open the **Virtual Router Configuration** page.
2. Select **Create** from the VRID and Interface drop-down menu.
3. Specify the VRID and the interface for the new virtual router.
4. Define the remaining fields as needed.
5. Click **Apply Changes**.

   The new virtual router is saved, and the device is updated.

   The configuration is saved, and the device is updated.

Configuring a Secondary IP Address

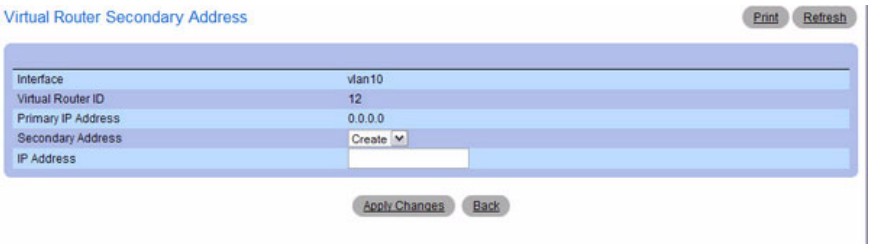
If you wish to configure a Secondary VRRP address, first configure one IP address (the primary address) for the VR. You can then add multiple Secondary addresses to that interface.

1. Open the **Router Configuration** page. Because you first configured the primary address, now the **Secondary IP Address** button appears at the bottom of the page.
2. Click the **Secondary IP Address** button.

   The **Virtual Router Secondary Address** page displays.

Downloaded from www.Manualslib.com manuals search engine

Figure 9-46. Virtual Router Secondary Address



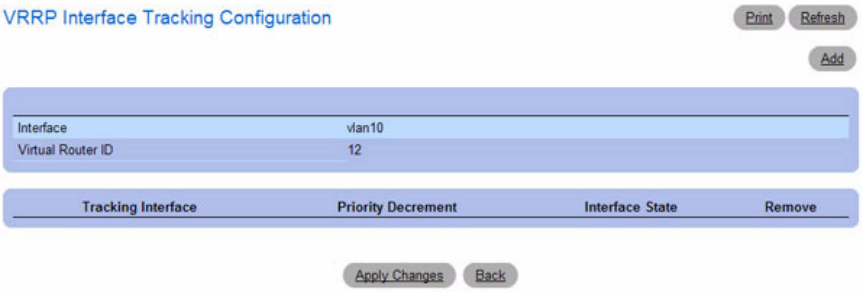
3. In the **Secondary Address** field, select **Create** to add a new secondary IP address, or select an existing secondary IP address to modify.
4. In the **IP Address** field, enter the secondary IP address.
5. Click **Apply Changes**.

Configuring VRRP Interface Tracking

1. Open the **VRRP Router Configuration** page.
2. Click **Track Interface**.

   The VRRP **Interface Tracking Configuration** page displays. From this page, you can add a new interface to track or remove a tracked interface.

Figure 9-47. VRRP Interface Tracking Configuration

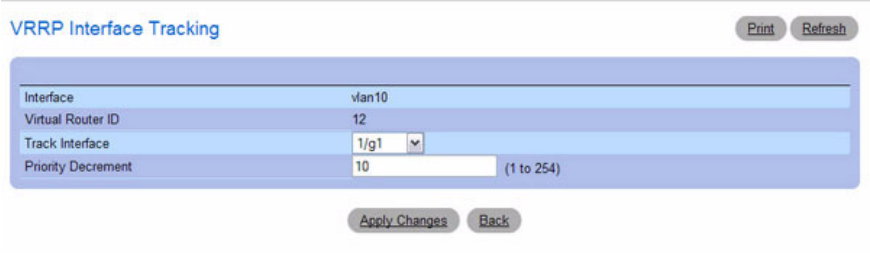


3. Click **Add**.

   The page refreshes, and the configuration fields appear.

Downloaded from www.Manualslib.com manuals search engine

Figure 9-48. Add VRRP Interface Tracking



4. Complete the fields as necessary.

   The Add VRRP Interface Tracking page contains the following fields.

   - **Interface** — The interface associated with the Virtual Router ID.
   - **Virtual Router ID** — The Virtual Router ID.
   - **Track Interface** — Select an interface for the VRRP router to track.
   - **Priority Decrement** — When a tracked interface goes down, the priority decrement specifies the amount that the router priority will be decreased. The valid range is 1 to 254. The default value is 10.

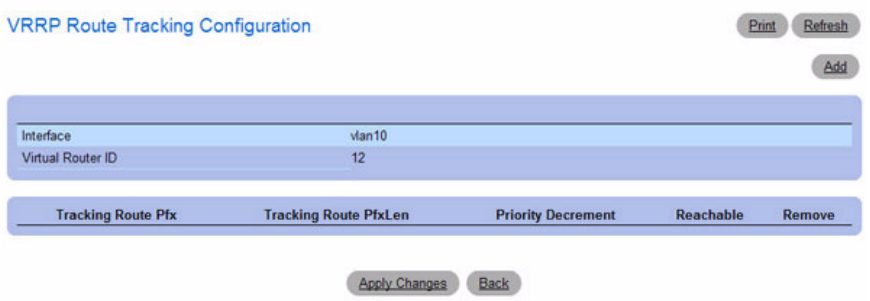
5. Click **Apply Changes** to update the switch.

Configuring VRRP Route Tracking

1. Open the VRRP **Router Configuration** page.
2. Click **Track Route**.

   The **VRRP Route Tracking Configuration** page displays. From this page, you can add a new route to track or remove a tracked route.

Figure 9-49. VRRP Route Tracking Configuration

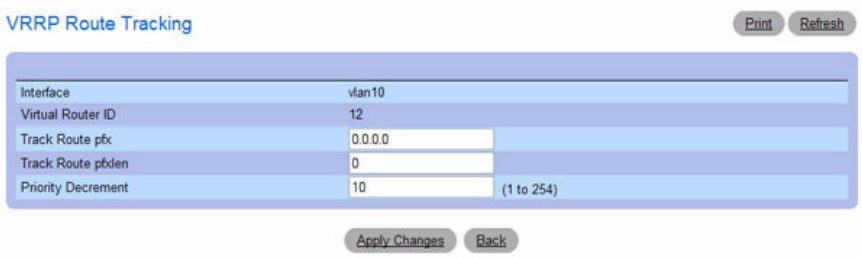


3. To add a VRRP tracking route, click **Add**.

   The page refreshes, and the configuration fields appear.

Downloaded from www.Manualslib.com manuals search engine

Figure 9-50. Add VRRP Route Tracking



4. Complete the fields as necessary.

   The **Add VRRP Route Tracking** page contains the following fields.

   - **Interface** — The interface associated with the Virtual Router ID.
   - **Virtual Router ID** — The Virtual Router ID.
   - **Track Route pfx**— Enter the destination prefix for the route to be tracked. Specify the prefix in dotted decimal format, for example 192.168.10.0
   - **Track Route pfxlen** — Enter the prefix length for the route to track.
   - **Priority Decrement** — When a tracked route becomes unreachable, the priority decrement specifies the amount that the router priority will be decreased. The valid range is 1 to 254. The default value is 10.

5. Click **Apply Changes** to update the switch.

Configuring a Virtual Router using the CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide:*

- Virtual Router Redundancy Protocol Commands

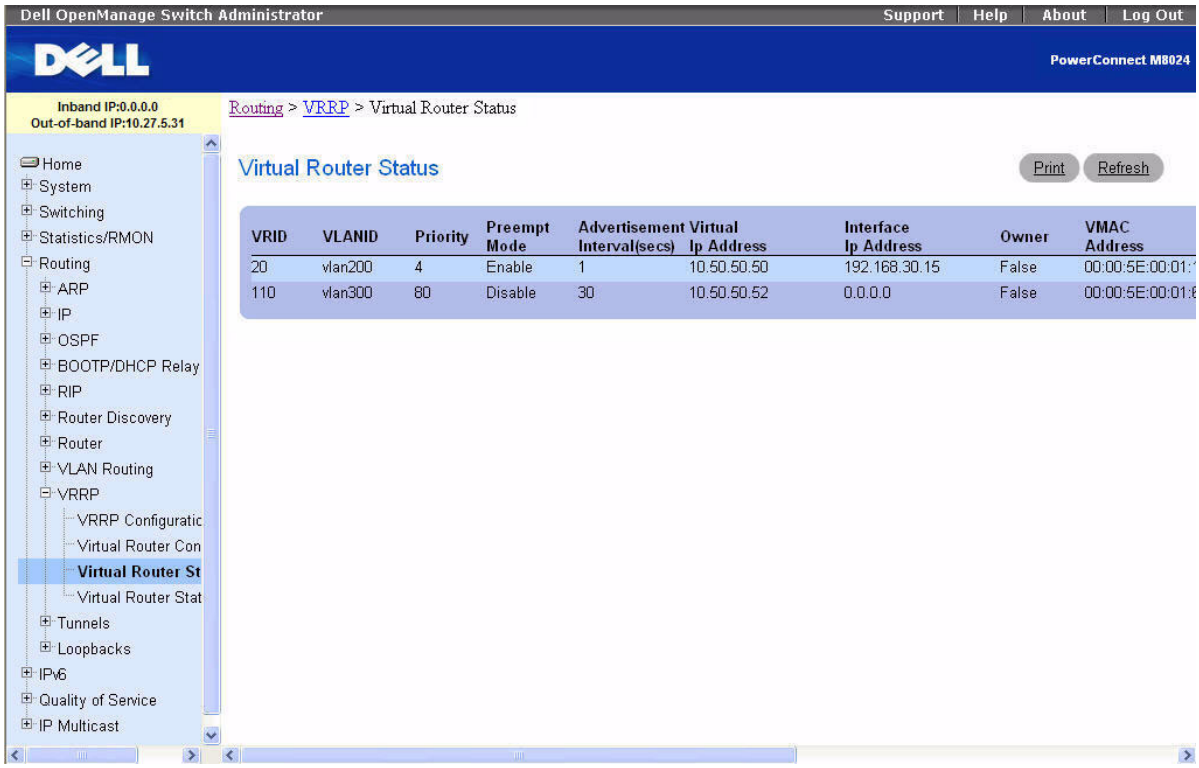
Downloaded from www.Manualslib.com manuals search engine

VRRP Virtual Router Status

Use the Virtual Router Status page to display virtual router status.

To display the page, click **Routing > VRRP > Virtual Router Status** in the tree view.

Figure 9-51. Virtual Router Status



The **Virtual Router Status** page displays the following fields:

- **VRID** — Virtual Router Identifier.
- **VLANID** - Indicates the interface associate with the VRID.
- **Priority** — The priority value used by the VRRP router in the election for the master virtual router.
- **Pre-empt Mode**
  - **Enable** — If the Virtual Router is a backup router it preempts the master router if it has a priority greater than the master virtual router's priority provided the master is not the owner of the virtual router IP address.
  - **Disable** — If the Virtual Router is a backup router it does not preempt the master router even if its priority is greater.
- **Advertisement Interval (secs)** — The time, in seconds, between the transmission of advertisement packets by this virtual router.
- **Virtual IP Address** — The IP Address associated with the Virtual Router.

Downloaded from www.Manualslib.com manuals search engine

- **Interface IP Address** — The actual IP Address associated with the interface used by the Virtual Router.
- **Owner** — Set to True if the Virtual IP Address and the Interface IP Address are the same, otherwise set to False. If this parameter is set to True, the Virtual Router is the owner of the Virtual IP Address, and always wins an election for master router when it is active.
- **VMAC Address** — The virtual MAC Address associated with the Virtual Router, composed of a 24-bit organizationally unique identifier, the 16-bit constant identifying the VRRP address block and the 8-bit VRID. The Virtual MAC address is 00:00:5e:00:01:XX where XX is the VRID.
- **Auth Type** — The type of authentication in use for the Virtual Router
  - None — Specifies that the authentication type is none.
  - Simple — Specifies that the authentication type is a simple text password.
- **State** — The current state of the Virtual Router:
  - Initialize
  - Master
  - Backup
- **Status** — The current status of the Virtual Router:
  - Inactive
  - Active
- **Secondary IP Address** — A secondary VRRP address configured for the primary VRRP.

Displaying Virtual Router Status using the CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide:*

- Virtual Router Redundancy Protocol Commands

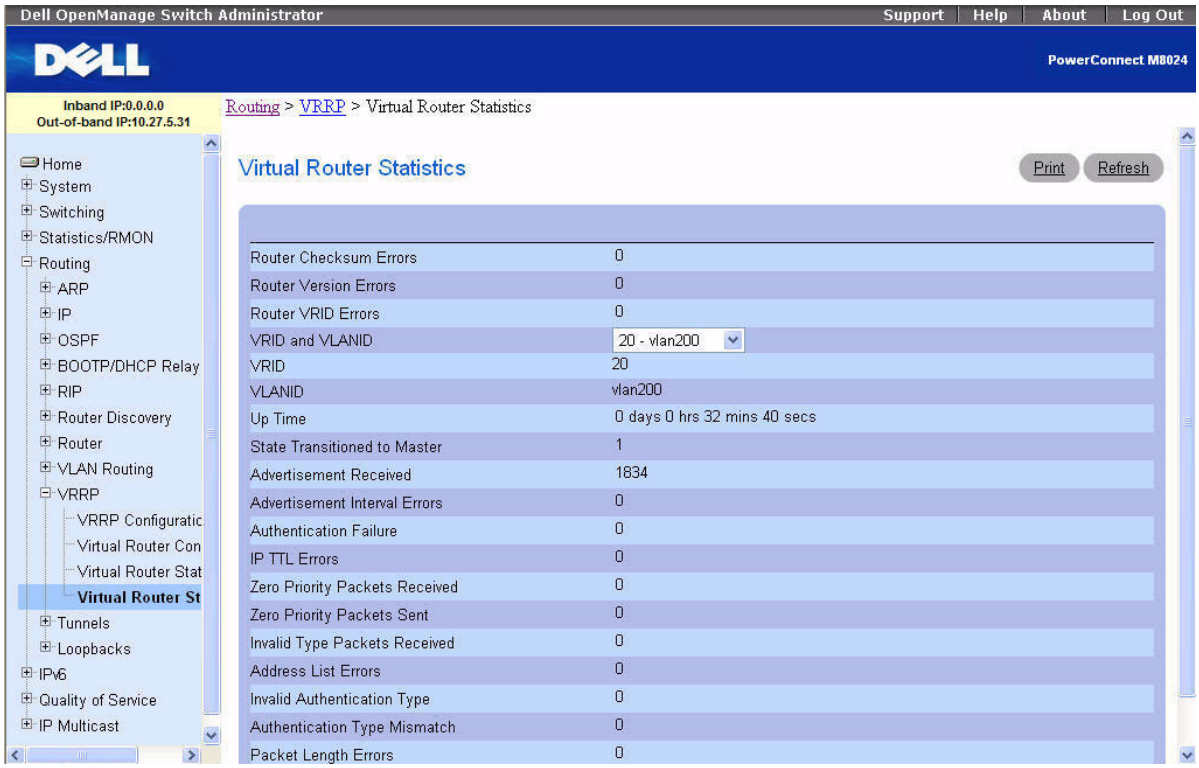
Downloaded from www.Manualslib.com manuals search engine

VRRP Virtual Router Statistics

Use the **Virtual Router Statistics** page to display statistics for a specified virtual router.

To display the page, click **Routing > VRRP > Virtual Router Statistics** in the tree view.

Figure 9-52. Virtual Router Statistics



The **Virtual Router Statistics** page contains the fields listed below. Many of the fields display only when there is a valid VRRP configuration.

- **Router Checksum Errors** — The total number of VRRP packets received with an invalid VRRP checksum value.
- **Router Version Errors** — The total number of VRRP packets received with an unknown or unsupported version number.
- **Router VRID Errors** — The total number of VRRP packets received with an invalid VRID for this virtual router.
- **VRID and VLAN ID** — Select the existing Virtual Router, listed by interface number and VRID, for which you want to display statistical information.
- **VRID** — the VRID for the selected Virtual Router.
- **VLAN ID** — The interface for the selected Virtual Router.

Downloaded from www.Manualslib.com manuals search engine

- **Up Time** — The time, in days, hours, minutes and seconds, that has elapsed since the virtual router transitioned to the initialized state.
- **State Transitioned to Master** — The total number of times that this virtual router's state has transitioned to Master.
- **Advertisement Received** — The total number of VRRP advertisements received by this virtual router.
- **Advertisement Interval Errors** — The total number of VRRP advertisement packets received for which the advertisement interval was different than the one configured for the local virtual router.
- **Authentication Failure** — The total number of VRRP packets received that did not pass the authentication check.
- **IP TTL Errors** — The total number of VRRP packets received by the virtual router with IP TTL (Time-To-Live) not equal to 255.
- **Zero Priority Packets Received** — The total number of VRRP packets received by the virtual router with a priority of 0.
- **Zero Priority Packets Sent** — The total number of VRRP packets sent by the virtual router with a priority of 0.
- **Invalid Type Packets Received** — The number of VRRP packets received by the virtual router with an invalid value in the Type field.
- **Address List Errors** — The total number of packets received for which the address list does not match the locally configured list for the virtual router.
- **Invalid Authentication Type** — The total number of packets received with an unknown authentication type.
- **Authentication Type Mismatch** — The total number of packets received with an authentication type different to the locally configured authentication method.
- **Packet Length Errors** — The total number of packets received with a packet length less than the length of the VRRP header.

Displaying Virtual Router Statistics

1. Open the **Virtual Router Statistics** page.
2. Select the virtual router for which you want to display statistical information from the **VRID** and **VLANID** field. This information displays only if there is a valid VRRP configuration.

Displaying Virtual Router Statistics using the CLI Command

For information about the CLI command that performs this function, see the following chapter in the *CLI Reference Guide:*

- Virtual Router Redundancy Protocol Commands

Downloaded from www.Manualslib.com manuals search engine

Tunnels

The PowerConnect M6220/M6348/M8024 switches support the creation, deletion, and management of tunnel interfaces. These are dynamic interfaces that are created and deleted through user-configuration. Each switch also supports the functionality of a 6to4 border router that connects a 6to4 site to a 6to4 domain. It sends and receives tunneled traffic from routers in a 6to4 domain that includes other 6to4 border routers and 6to4 relay routers.

There are two classes of tunnels that facilitate the transition of IPv4 networks to IPv6 networks: configured and automatic. The distinction is that configured tunnels are explicitly configured with a destination or endpoint of the tunnel. Automatic tunnels, in contrast, infer the endpoint of the tunnel from the destination address of packets routed into the tunnel.

The PowerConnect M6220/M6348/M8024 supports point-to-point tunnels. Point-to-point interfaces provide for routing based only on the interface (an explicit next-hop address need not be specified), and allow for the definition of unnumbered interfaces.

The **Tunnels** menu page contains links to web pages that configure and display tunnel parameters and data. To display this page, click **Routing > Tunnels** in the tree view. Following are the web pages accessible from this menu page:

- Tunnels Configuration
- Tunnels Summary

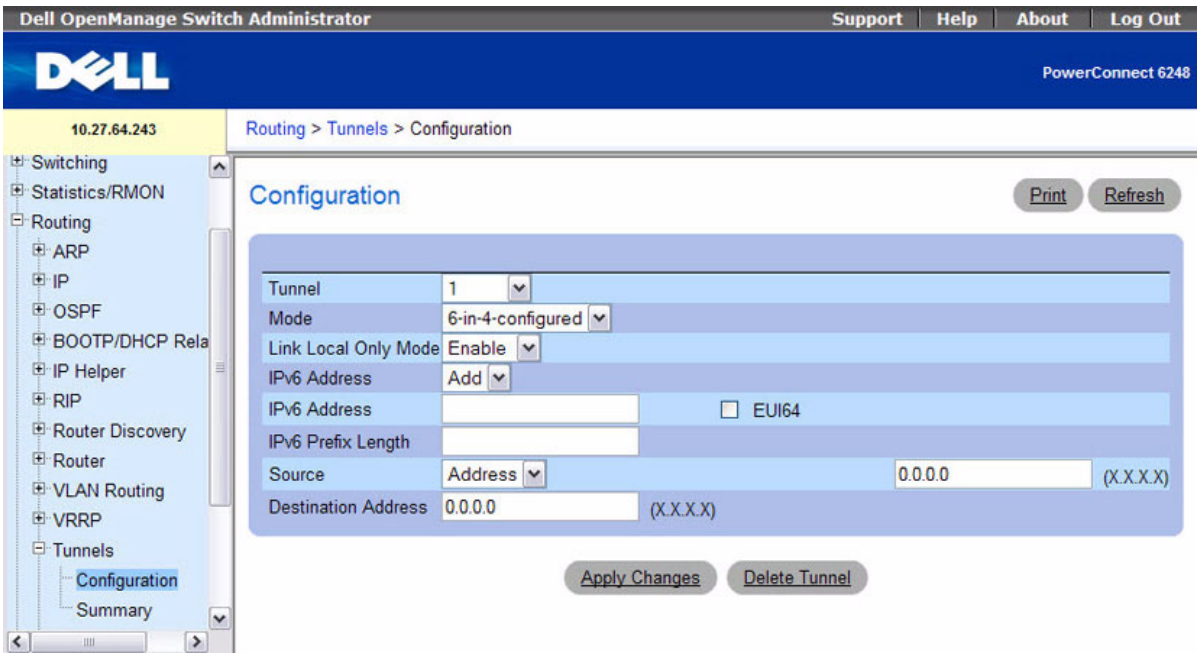
Downloaded from www.Manualslib.com manuals search engine

Tunnels Configuration

Use the **Tunnels Configuration** page to create, configure, or delete a tunnel.

To display the page, click **Routing > Tunnels > Configuration** in the tree view.

Figure 9-53. Tunnels Configuration



The **Tunnels Configuration** page contains the following fields:

- **Tunnel** — Use the drop-down menu to select from the list of currently configured tunnel IDs. **Create** is also a valid choice if the maximum number of tunnel interfaces has not been created.
- **Tunnel ID** — When Create is chosen from the tunnel selector this list of available tunnel IDs becomes visible. You must select a tunnel ID to associate with the new tunnel and click **Apply Changes** before the remaining fields on the page display.
- **Mode** — Selector for the Tunnel mode, which can be one of the following:
  - **6-in-4-configured** — The 6in4 tunnel mode is configured rather than automatic.
  - **6-to-4** — 6to4 tunnels are automatically formed IPv4 tunnels carrying IPv6 traffic. The automatic tunnel's IPv4 destination address is derived from the 6to4 IPv6 address of the tunnel's nexthop. The switch supports the functionality of a 6to4 border router that connects a 6to4 site to a 6to4 domain. It sends/receives tunneled traffic from routers in a 6to4 domain that includes other 6to4 border routers and 6to4 relay routers.
- **Link Local Only Mode** — Enable IPv6 on this interface using the Link Local address. This option is only configurable prior to specifying an explicit IPv6 address.

Downloaded from www.Manualslib.com manuals search engine

- **IPv6 Address** —Select an IPv6 address for the selected Tunnel interface. **Add** is also a valid choice if the maximum number of addresses has not been configured.
- **IPv6 Address** — When **Add** is chosen from the IPv6 Address drop-down menu, this IPv6 address input field becomes visible. The Address must be entered in the format prefix/length.

  You also have the option to specify the 64-bit extended unique identifier (EUI-64).
- **IPv6 Prefix Length** — Specify the IPv6 prefix length.
- **Source** — Select the desired source, IPv4 Address or Interface. If Address is selected, the source address for this tunnel must be entered in dotted decimal notation. If Interface is selected the source interface for this tunnel must be selected. The address associated with the selected interface is used as the source address.
- **Destination Address** — The IPv4 destination address for this tunnel in dotted decimal notation.

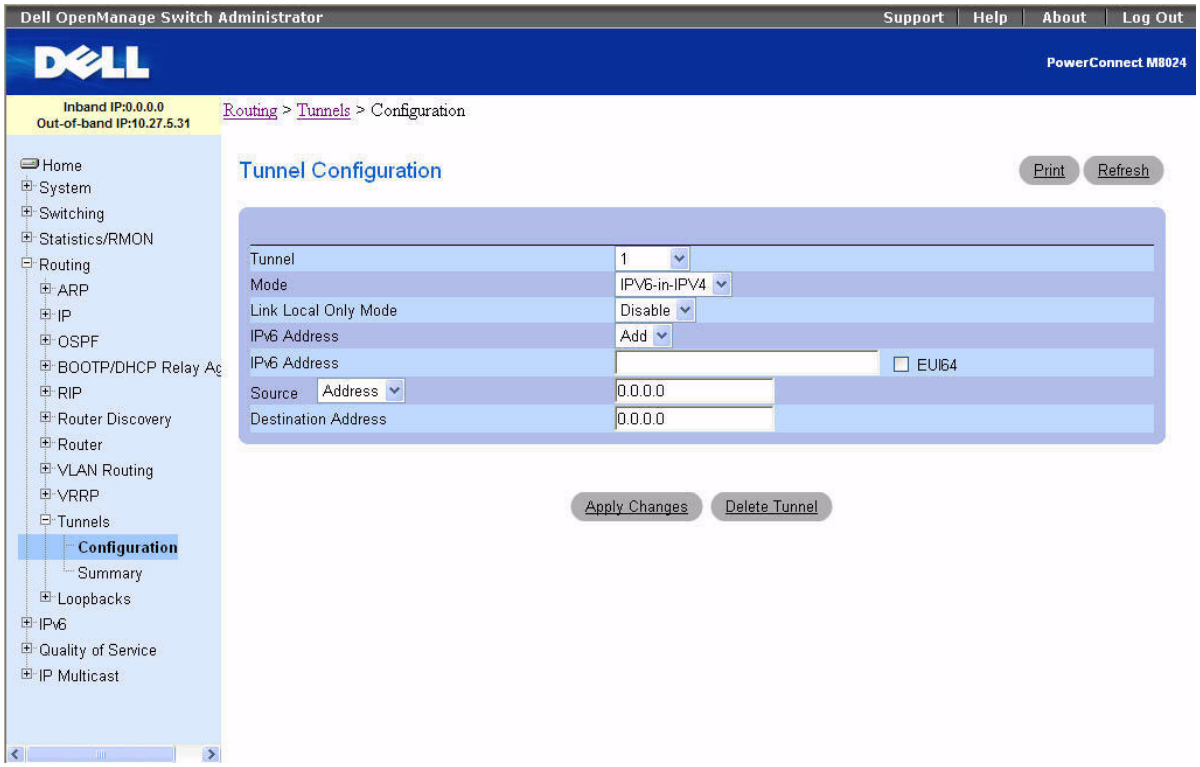
Creating a New Tunnel

1. Open the **Tunnels Configuration** page.
2. Select **Create** from the **Tunnel** drop-down menu.
3. Specify an ID to use in the **Tunnel ID** field.
4. Click **Apply Changes**.

   The Tunnel ID field is removed, and the remaining tunnel fields display.

Downloaded from www.Manualslib.com manuals search engine

Figure 9-54. Tunnels Configuration - Entry



5. Configure the fields as needed.
6. Enter desired values in the remaining fields.
7. Click **Apply Changes**.

   The new tunnel is saved, and the device is updated.

Modifying an Existing Tunnel

1. Open the **Tunnels Configuration** page.
2. Specify the tunnel to modify in the **Tunnel** drop-down menu.
3. Change field values as desired in the remaining fields.
4. Click **Apply Changes**.

   The new configuration is saved, and the device is updated.

Downloaded from www.Manualslib.com manuals search engine

Removing a Tunnel

1. Open the **Tunnels Configuration** page.
2. Specify the tunnel to remove in the **Tunnel** drop-down menu.
3. Click **Delete Tunnel**.

   The tunnel is deleted, and the device is updated.

Configuring a Tunnel using CLI Commands

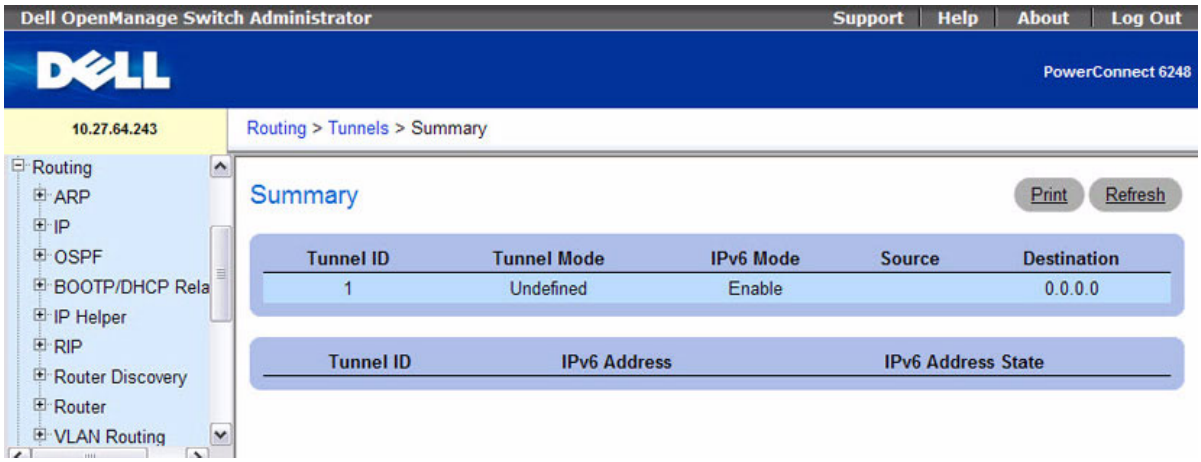
For information about the CLI command that performs this function, see the following chapter in the *CLI Reference Guide:*

- Tunnel Interface Commands

Tunnels Summary

Use the **Tunnels Summary** page to display a summary of configured tunnels. To display the page, click **Routing** > **Tunnels** > **Summary** in the tree view.

Figure 9-55. Tunnels Summary



The **Tunnels Summary** page contains the following fields:

- **Tunnel ID** — The Tunnel ID.
- **Tunnel Mode** — The corresponding mode of the Tunnel.
- **IPv6 Mode** — Shows whether IPv6 is enabled on the tunnel.
- **Source** — The corresponding Tunnel Source Address. In the case where an interface has been configured both the interface and the address are displayed. If the source interface has no address configured then nothing is displayed in place of the address.
- **Destination** — The corresponding Tunnel Destination Address.
- **Tunnel ID** — The Tunnel ID.

Downloaded from www.Manualslib.com manuals search engine

- **IPv6 Address** — The IPv6 Address(es) of the Tunnel.

IPv6 Address State — Shows whether the address is active.

Displaying Tunnels Summary using the CLI Command

For information about the CLI command that performs this function, see the following chapter in the *CLI Reference Guide:*

- Tunnel Interface Commands

Loopbacks

The PowerConnect M6220/M6348/M8024 provides for the creation, deletion, and management of loopback interfaces. They are dynamic interfaces that are created and deleted through user-configuration. The PowerConnect M6220/M6348/M8024 supports multiple loopback interfaces.

A loopback interface is always expected to be up. As such, it provides a means to configure a stable IP address on the device that may be referred to by other switches. This interface provides the source address for sent packets and can receive both local and remote packets. It is typically used by routing protocols.

The loopback does not behave like the network port on Switching systems. In particular, there are no neighbors on a loopback interface. It is a pseudo-device for assigning local addresses so that the router can be communicated with by this address, which is always up and can receive traffic from any of the existing active interfaces. Thus, given reachability from a remote client, the address of the loopback can be used to communicate with the router through various services such as telnet and SSH. In this way, the address on a loopback behaves identically to any of the local addresses of the router in terms of the processing of incoming packets.

The **Loopbacks** menu page contains links to web pages that configure and display loopback parameters and data. To display this page, click **Routing > Loopbacks** in the tree view. Following are the web pages accessible from this menu page:

- Loopbacks Configuration
- Loopbacks Summary

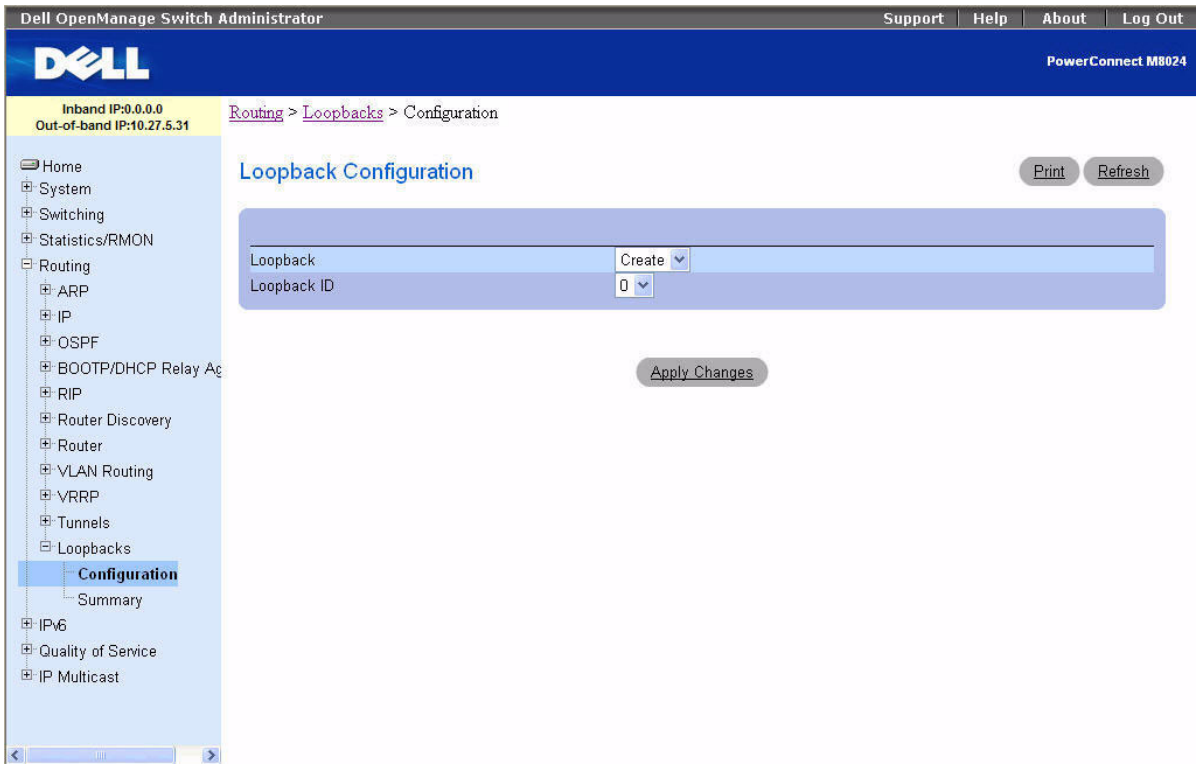
Downloaded from www.Manualslib.com manuals search engine

Loopbacks Configuration

Use the **Loopbacks Configuration** page to create, configure, or remove loopback interfaces. You can also set up or delete a secondary address for a loopback.

To display the page, click **Routing > Loopbacks > Configuration** in the tree view.

Figure 9-56. Loopback Configuration



The **Loopbacks Configuration** pages contain the following fields:

- **Loopback** — Use the drop-down menu to select from the list of currently configured loopback interfaces. Create is also a valid choice if the maximum number of loopback interfaces has not been created.
- **Loopback ID** — When Create is selected in the Loopback field, this list of available loopback ID's displays.
- **Protocol** — Select IPv4 or IPv6 to configure the corresponding attributes on the loopback interface. The protocol selected affects the fields that are displayed on this page.
- **Link Local Only Mode** — Enable IPv6 on this interface using the Link Local address. This option only displays when the Protocol specified is IPv6, and is only configurable prior to specifying an explicit IPv6 address.

Downloaded from www.Manualslib.com manuals search engine

- **IPv6 Address** — Select list of configured IPv6 addresses for the selected Loopback interface. Add is also a valid choice if the maximum number of addresses has not been configured. This option only displays when the Protocol specified is IPv6.
- **IPv6 Address** — When Add is chosen from the IPv6 Address selector this IPv6 address input field becomes visible. Enter the address in the format of prefix/length. This option only displays when the Protocol specified is IPv6.
- **EU164** — You also have the option to specify the 64-bit extended unique identifier (EUI-64). This option only displays when the Protocol specified is IPv6.
- **IPv4 Address** — The primary IPv4 address for this interface in dotted decimal notation. This option only displays when the Protocol specified is IPv4.
- **IPv4 Subnet Mask** — The primary IPv4 subnet mask for this interface in dotted decimal notation. This option only displays when the Protocol specified is IPv4.

The following fields display when a primary address is configured. You can configure multiple secondary addresses.

- **Secondary Address** — Select a configured IPv4 secondary address for the selected Loopback interface from the drop-down menu. A new address can be entered in the Secondary IP Address field by selecting Add Secondary IP Address here (if the maximum number of secondary addresses has not been configured). A primary address must be configured before a secondary address can be added.
- **Secondary IP Address** — The secondary IP address for this interface in dotted decimal notation. This input field is visible only when Add Secondary is selected.
- **Secondary Subnet Mask** — The secondary subnet mask for this interface in dotted decimal notation. This input field is visible only when Add Secondary is selected.

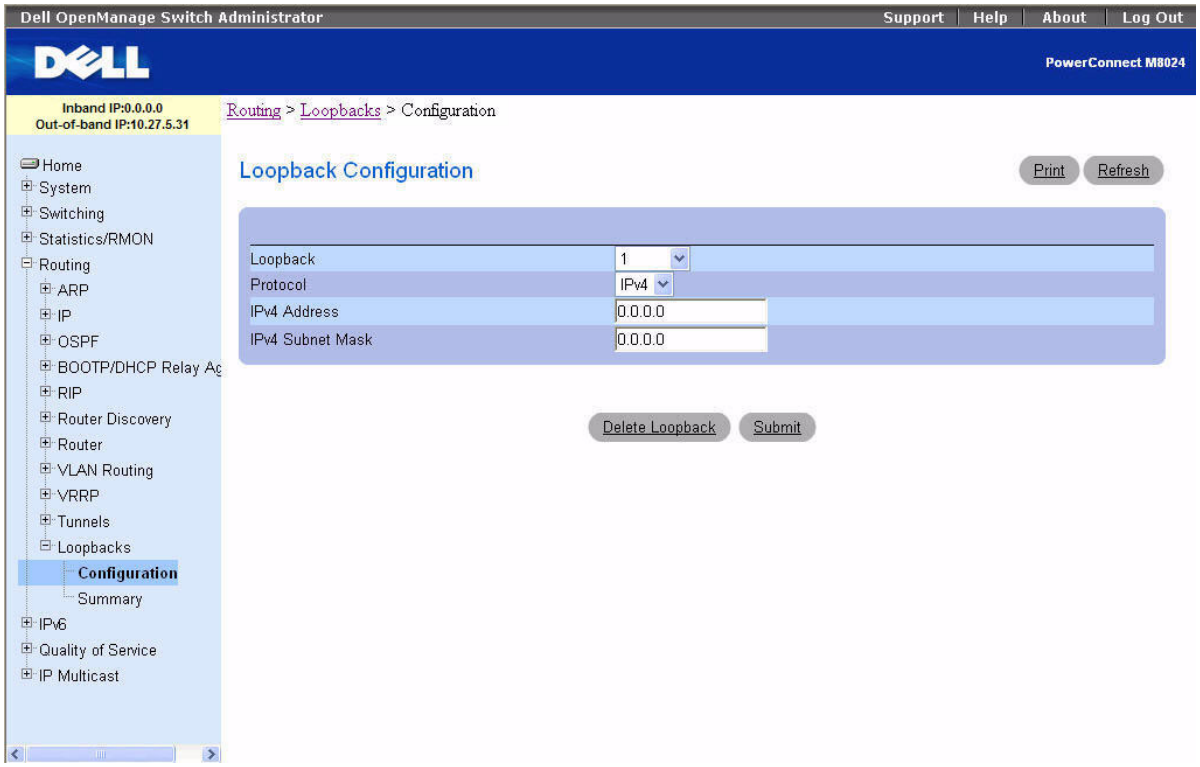
Creating a New Loopback (IPv4)

1. Open the **Loopbacks Configuration** page.
2. Select **Create** from the **Loopback** drop-down menu.
3. Specify an ID to use in the **Loopback ID** field.
4. Click **Apply Changes**.

   The Loopback ID field goes away, and the remaining loopback fields display.

Downloaded from www.Manualslib.com manuals search engine

Figure 9-57. Loopbacks Configuration - IPv4 Entry

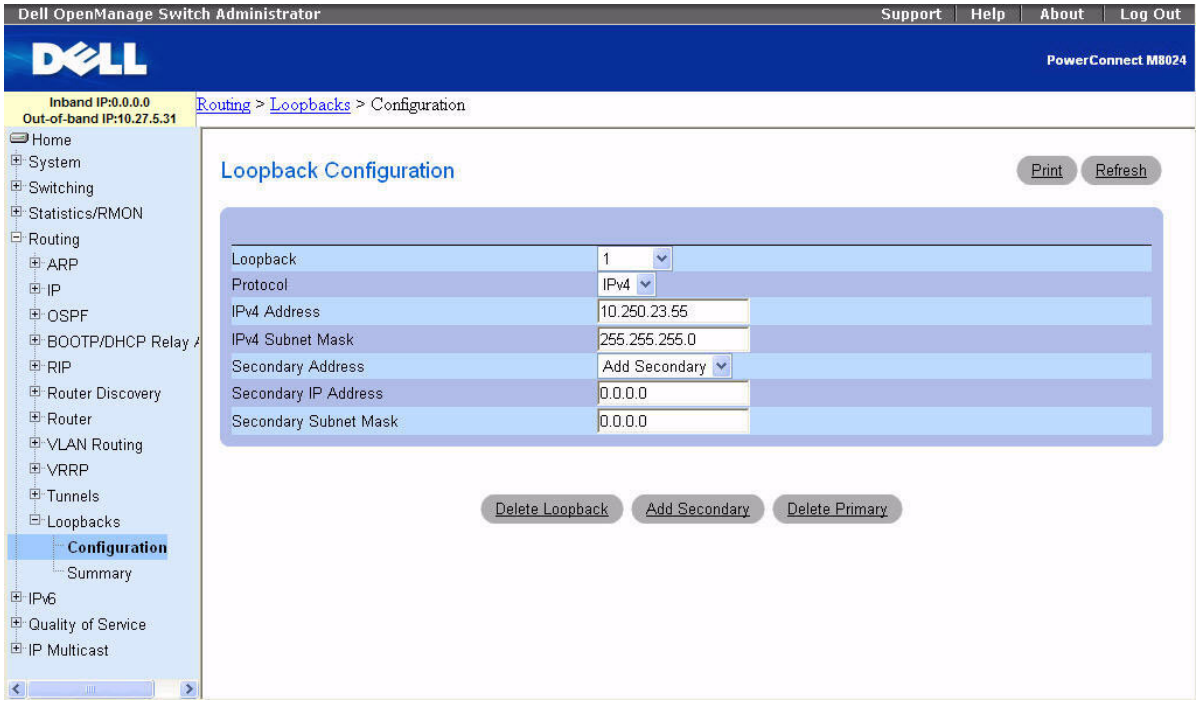


5. Enter **IPv4** in the **Protocol** field.
6. Enter desired values in the remaining fields.
7. Click **Submit**.

   The new loopback is saved, and the webpage reappears showing secondary address configuration fields.

Downloaded from www.Manualslib.com manuals search engine

Figure 9-58. Loopback Configuration - Add Secondary Address



8. Complete the **Secondary Address**, **Secondary IP Address**, and **Secondary Subnet Mask** fields.
9. Click the **Add Secondary** button. The secondary address is saved, and the webpage reappears showing the primary and secondary loopback addresses.

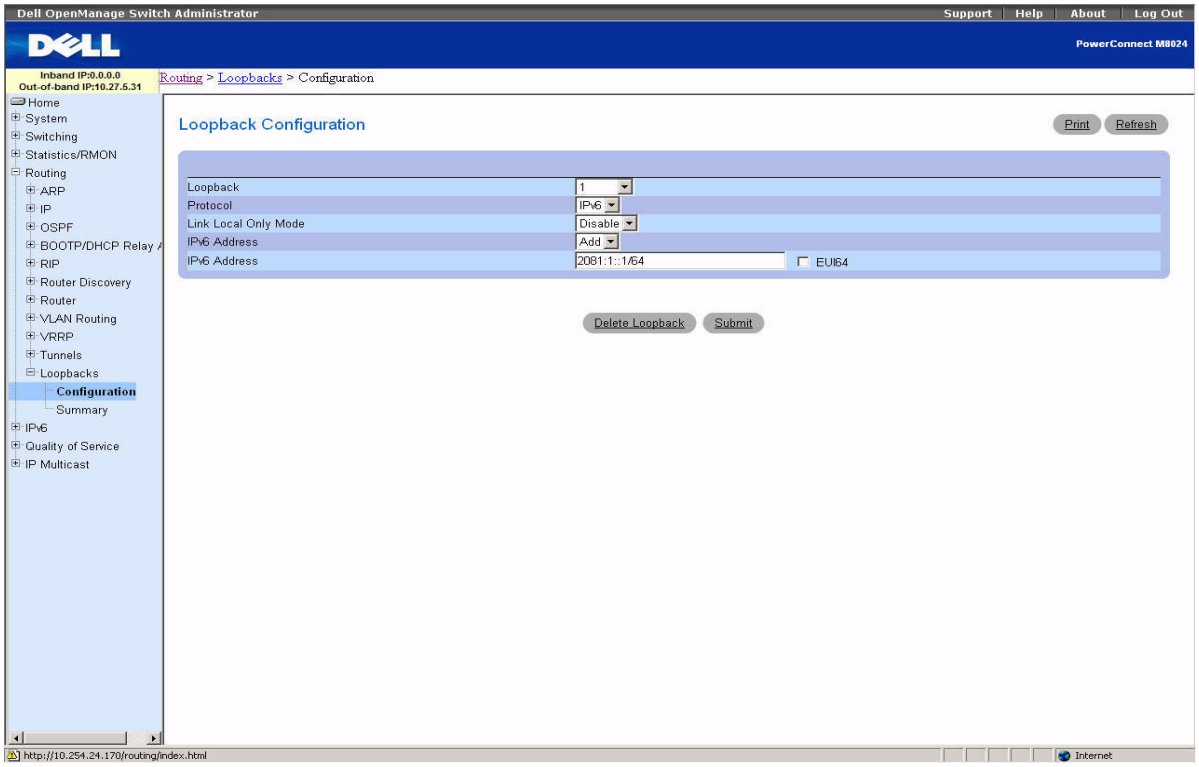
Creating a New Loopback (IPv6)

1. Open the **Loopbacks Configuration** page.
2. Select **Create** from the **Loopback** drop-down menu.
3. Specify an ID to use in the **Loopback ID** field.
4. Click Apply Changes.

The Loopback ID field goes away, and the remaining loopback fields display.

Downloaded from www.Manualslib.com manuals search engine

Figure 9-59. Loopbacks Configuration - IPv6 Entry



5. Choose **IPv6** from the drop-down box in the **Protocol** field.
6. Add the **IPv6 Address**.
7. Enter desired values in the remaining fields.
8. Click **Submit**.

   The new loopback is saved, and the device is updated.

Configuring an Existing Loopback

1. Open the **Loopback Configuration** page.
2. Specify the loopback to configure in the **Loopback** drop-down menu.
3. Change field values as desired in the remaining fields.
4. Click **Apply Changes**.

   The new configuration is saved, and the device is updated.

Downloaded from www.Manualslib.com manuals search engine

Removing a Loopback

1. Open the **Loopback Configuration** page.
2. Specify the loopback to remove in the **Loopback** drop-down menu.
3. Click **Delete Loopback**.

   The loopback is deleted, and the device is updated.

Removing a Secondary Address

1. Open the **Loopback Configuration** page.
2. Specify the loopback to be affected.
3. Specify the secondary address to be removed.
4. Click **Delete Selected Secondary**.

   The secondary address is deleted, and the device is updated.

Configuring a Loopback using CLI Commands

For information about the CLI commands that perform this function, see the following chapters in the *CLI Reference Guide:*

- Loopback Interface Commands
- IP Addressing Commands
- IPv6 Routing Commands

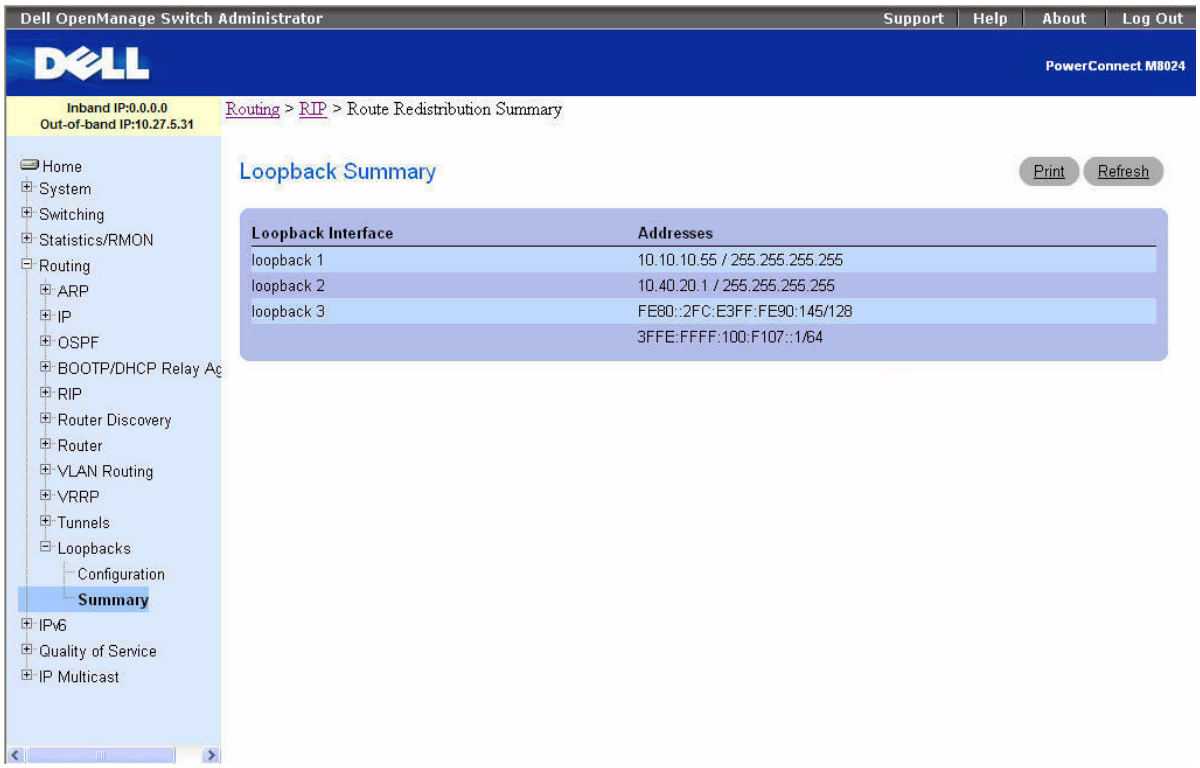
Downloaded from www.Manualslib.com manuals search engine

Loopbacks Summary

Use the **Loopbacks Summary** page to display a summary of configured loopbacks.

To display the page, click **Routing > Loopbacks > Summary** in the tree view.

Figure 9-60. Loopbacks Summary



The **Loopbacks Summary** page displays the following fields:

- **Loopback Interface** — The ID of the configured loopback interface.
- **Addresses** — A list of the addresses configured on the loopback interface.

Displaying the Loopbacks Summary using the CLI Command

For information about the CLI command that performs this function, see the following chapter in the *CLI Reference Guide:*

- Loopback Interface Commands

Downloaded from www.Manualslib.com manuals search engine

10

Configuring IPv6

Overview

IPv6 is the next generation of the Internet Protocol. With 128-bit addresses, versus 32-bit addresses for IPv4, IPv6 solves the address depletion issues seen with IPv4 and removes the requirement for Network Address Translation (NAT), which is used in IPv4 networks to reduce the number of globally unique IP addresses required for a given network. Its aggregate addresses can dramatically reduce the size of the global routing table through well known address combinations. Security is more integrated and network configuration is simplified yet more flexible.

On the PowerConnect M6220/M6348/M8024, IPv6 coexists with IPv4. As with IPv4, IPv6 routing can be enabled on loopback and VLAN interfaces. Each L3 routing interface can be used for IPv4, IPv6, or both. IP protocols running over L3 (for example, UDP and TCP) do not change with IPv6. For this reason, a single CPU stack is used for transport of both IPv4 and IPv6, and a single sockets interface provides access to both. Routing protocols are capable of computing routes for one or both IP versions.

The **IPv6** menu page contains links to the following features:

- Global Configuration
- Interface Configuration
- Interface Summary
- IPv6 Statistics
- IPv6 Neighbor Table
- DHCPv6
- OSPFv3
- IPv6 Routes

Note: CLI commands are not available for all the IPv6 pages.

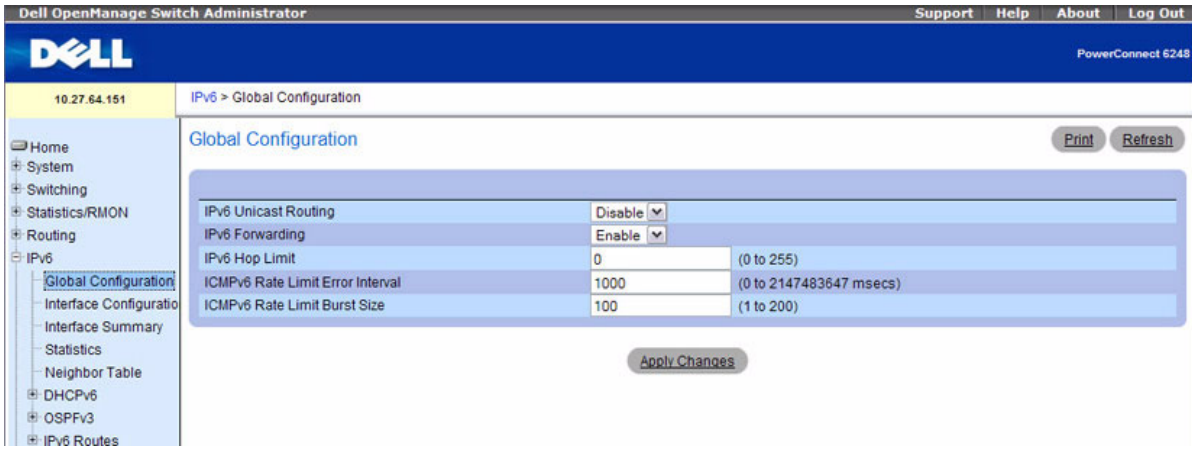
Downloaded from www.Manualslib.com manuals search engine

Global Configuration

Use the **Global Configuration** page to enable IPv6 forwarding on the router, enable the forwarding of IPv6 unicast datagrams, and configure global IPv6 settings.

To display the page, click **IPv6 > Global Configuration** in the tree view.

Figure 10-1. IPv6 Global Configuration



The **IPv6 Global Configuration** page contains the following fields:

- **IPv6 Unicast Routing** — Globally enable or disable IPv6 unicast routing on the router. The default is Disable.
- **IPv6 Forwarding** — Enable or disable forwarding of IPv6 frames on the router. The default is Enable.
- **IPv6 Hop Limit** — Specifies the TTL value for the router.
- **ICMPv6 Rate Limit Error Interval** — To control the ICMPv6 error packets, specify the number of ICMP error packets that are allowed per burst interval. The default Rate Limit is 100 packets per second. In other words, the burst interval is 1000 milliseconds. To disable ICMP Rate Limiting, set this value to zero. The Error Interval range is 0–2147483647.

ICMPv6 Rate Limit Burst Size — To control the ICMPv6 error packets, specify the number of ICMP error packets that are allowed per burst interval. The default Burst Size is 100 packets. The valid Burst Size must be in the range of 1 to 200.

Configuring IPv6 Parameters

1. Open the **IPv6 Global Configuration** page.
2. Enable or disable unicast routing from the drop-down menu.
3. Enable or disable IPv6 frames forwarding from the drop-down menu.
4. Click **Apply Changes**.

   Settings are saved, and the device is updated.

Downloaded from www.Manualslib.com manuals search engine

Configuring IPv6 using the CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

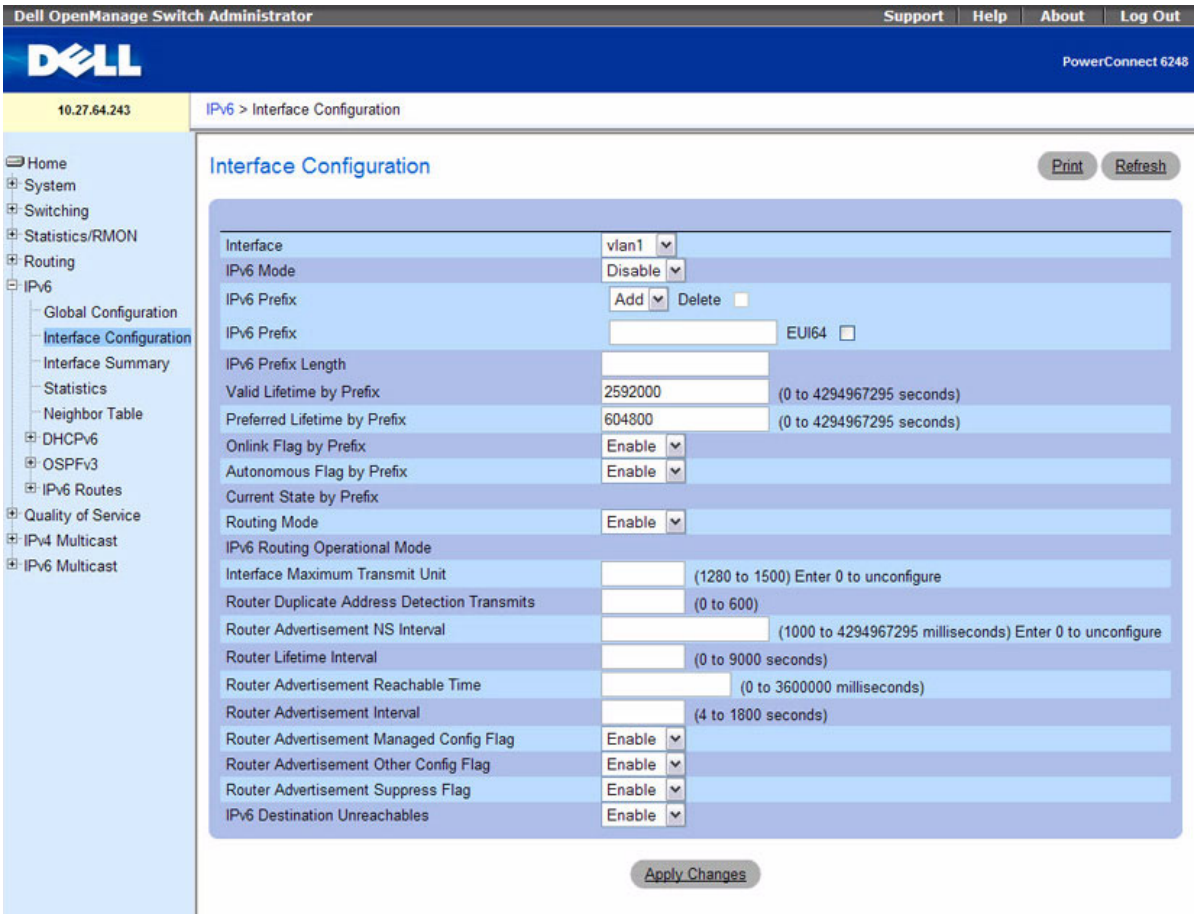
- IPV6 Routing Commands

Interface Configuration

Use the **Interface Configuration** page to configure IPv6 interface parameters. This page has been updated to include the IPv6 Destination Unreachables field.

To display the page, click **IPv6 > Interface Configuration** in the tree view.

Figure 10-2. IPv6 Interface Configuration



Downloaded from www.Manualslib.com manuals search engine

The **IPv6 Interface Configuration** page contains the following fields:

- **Interface** — Selects the interface to be configured. When the selection is changed, a screen refresh occurs, causing all fields to be updated for the newly selected interface. Shows only routing-enabled interfaces and tunnels.
- **IPv6 Mode** — When IPv6 mode is enabled, interface is capable of IPv6 operation without a global address. In this case, an EUI-64 based link-local address is used. This selector lists the two options for IPv6 mode: **Enable** and **Disable**. Default value is **Disable**.
- **IPv6 Prefix** — Choose to **Add** or **Delete** an IPv6 prefix on this interface. If adding a prefix, specify that prefix in the following **IPv6 Prefix** field. Checking **Delete** causes deletion of a displayed IPv6 Prefix.
- **IPv6 Prefix** — Specifies the IPv6 prefix for an interface. When the selection is changed, the screen is refreshed and valid lifetime, preferred lifetime, on-link flag, and autonomous flag fields are updated for the selected IPv6 address.
- **EUI-64** — If checked, specifies 64-bit unicast prefix.
- **IPv6 Prefix Length** — Specifies the IPv6 prefix length.
- **Valid Lifetime by Prefix** — The value, in seconds, to be placed in the **Valid Lifetime** field of the **Prefix Information** option in a router advertisement. The prefix is valid for on-link determination for this length of time. Hosts that generate an address from this prefix using stateless address auto-configuration can use those addresses for this length of time. An auto-configured address older than the preferred lifetime but younger than the valid lifetime are considered to be deprecated addresses. As defined by RFC 2462, a deprecated address is an address assigned to an interface whose use is discouraged, but not forbidden. A deprecated address should no longer be used as a source address in new communications, but packets sent from or to deprecated addresses are delivered as expected. A deprecated address may continue to be used as a source address in communications where switching to a preferred address causes hardship to a specific upper-layer activity (for example, an existing TCP connection). The valid range is from 0 to 4,294,967,295 seconds.
- **Preferred Lifetime by Prefix** — The value, in seconds, to be placed in the **Preferred Lifetime** in the **Prefix Information** option in a router advertisement. Addresses generated from a prefix using stateless address autoconfiguration remain preferred for this length of time. As defined by RFC 2462, a preferred address is "an address assigned to an interface whose use by upper layer protocols is unrestricted. Preferred addresses may be used as the source (or destination) address of packets sent from (or to) the interface." The range is from 0 to 4,294,967,295 seconds.
- **Onlink Flag by Prefix** — Specifies the selected prefix that can be used for on-link determination. Default value is Enable. This selector lists the two options for on-link flag: Enable and Disable.
- **Autonomous Flag by Prefix** — Specifies the selected prefix that can be used for autonomous address configuration. Default value is Disable. This selector lists the two options for autonomous flag: Enable and Disable.
- **Current State by Prefix** — Interface Operational status for selected IPv6 prefix.
- **Routing Mode** — Specifies the routing mode of an interface. This selector lists the two options for routing mode: Enable and Disable. Default value is Disable.

Downloaded from www.Manualslib.com manuals search engine

- **IPv6 Routing Operational Mode** — Displays the operational state of an interface.
- **Interface Maximum Transmit Unit** — Specifies the maximum transmit unit on an interface. If the value is 0 then this interface is not enabled for routing. It is not valid to set this value to 0 if routing is enabled. The valid range of MTU is 1280 to 1500.
- **Router Duplicate Address Detection Transmits** — Specifies the number of duplicate address detections transmits on an interface. DAD transmits values must be in the range of 0 to 600.
- **Router Advertisement NS Interval** — Specifies retransmission time field of router advertisement sent from the interface. A value of 0 means the interval is not specified for this router. The range of neighbor solicit interval is 1000 to 4294967295.
- **Router Lifetime Interval** — Specifies the router advertisement lifetime field sent from the interface. This value must be greater than or equal to the maximum advertisement interval. 0 means do not use the router as the default router. The range of router lifetime is 0 to 9000.
- **Router Advertisement Reachable Time** — Specifies the router advertisement time to consider neighbor reachable after the neighbor discovery (ND) confirmation. The range of reachable time is 0 to 3600000.
- **Router Advertisement Interval** — Specifies the maximum time allowed between sending router advertisements from the interface. The default value is 600. the range of maximum advertisement interval is 4 to 1800.
- **Router Advertisement Managed Config Flag** — Specifies the router advertisement managed address configuration flag. When true, the end nodes use DHCPv6. When false, the end nodes auto configure the addresses. The default value of managed flag is Disable.
- **Router Advertisement Other Config Flag** — Specifies the router advertisement other stateful configuration flag. The default value of other config flag is Disable.
- **Router Advertisement Suppress Flag** — Specifies the router advertisement suppression on an interface. The default value of suppress flag is Disable.
- **IPv6 Destination Unreachables** — Indicates whether the interface sends (Enabled) or suppresses (Disabled) ICMPv6 unreachable messages. This field also applies to tunnels.

Configuring IPv6 Interface

1. Open the **IPv6 Interface Configuration** page.
2. Modify the fields as needed.
3. Click **Apply Changes**.

   The IPv6 interface modifications are saved, and the device is updated.

Configuring IPv6 Interface with the CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- IPV6 Routing Commands

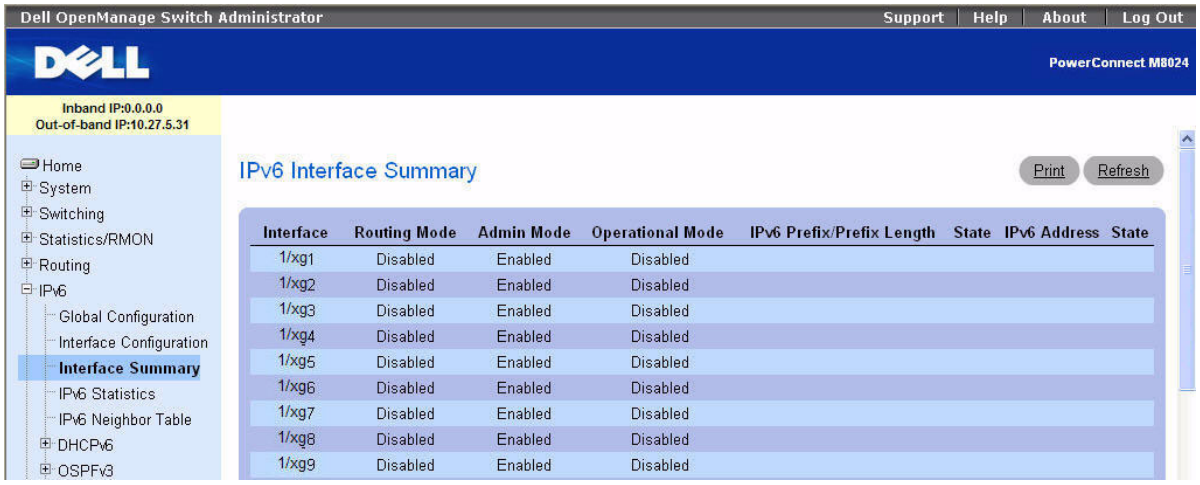
Downloaded from www.Manualslib.com manuals search engine

Interface Summary

Use the **Interface Summary** page to display settings for all IPv6 interfaces.

To display the page, click **IPv6 > Interface Summary** in the tree view.

Figure 10-3. IPv6 Interface Summary



The **IPv6 Interface Summary** page contains the following fields:

Interface — Specifies the interface whose settings are displayed in the current table row.

Routing Mode — Specifies routing mode of the interface.

Admin Mode — Specifies administrative mode of the interface.

Operational Mode — Specifies operational mode of the interface.

IPv6 Prefix/PrefixLength — Specifies configured IPv6 addresses on the interface.

State — Specifies whether the interface is active or not.

Displaying IPv6 Interface Summary using the CLI Command

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- IPV6 Routing Commands

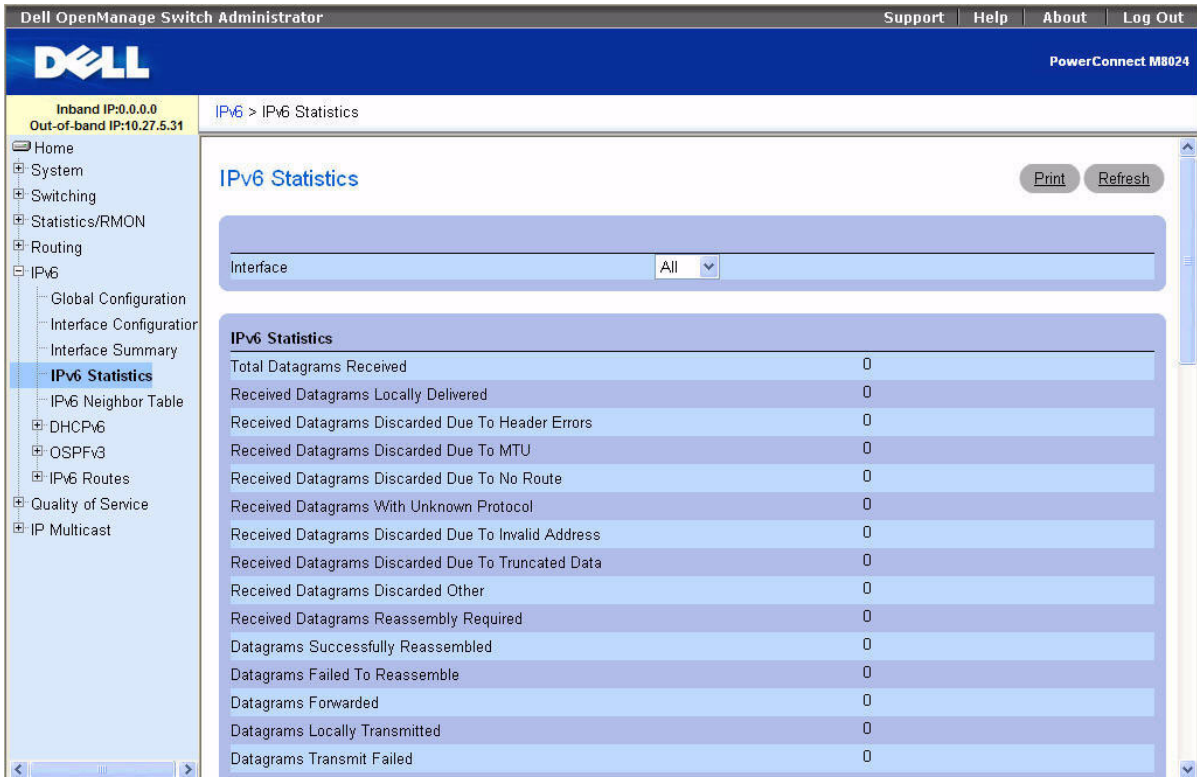
Downloaded from www.Manualslib.com manuals search engine

IPv6 Statistics

Use the **IPv6 Statistics** page to display IPv6 traffic statistics for one or all interfaces.

To display the page, click **IPv6 > IPv6 Statistics** in the tree view.

Figure 10-4. IPv6 Statistics



The **IPv6 Statistics** page contains the following fields:

- **Interface** — Selects the interface for which statistics are displayed. When the selection is changed, a screen refresh occurs, causing all fields to be updated for the newly selected interface.

IPv6 Statistics

- **Total Datagrams Received** — The total number of input datagrams received by the interface, including those received in error.
- **Received Datagrams Locally Delivered** — The total number of datagrams successfully delivered to IPv6 user-protocols (including ICMP). This counter is incremented at the interface to which these datagrams were addressed, which might not be necessarily the input interface for some of the datagrams.
- **Received Datagrams Discarded Due To Header Errors** — The number of input datagrams discarded due to errors in their IPv6 headers, including version number mismatch, other format errors, hop count exceeded, errors discovered in processing their IPv6 options, etc.

Downloaded from www.Manualslib.com manuals search engine

- **Received Datagrams Discarded Due To MTU** — The number of input datagrams that could not be forwarded because their size exceeded the link MTU of outgoing interface.
- **Received Datagrams Discarded Due To No Route** — The number of input datagrams discarded because no route could be found to transmit them to their destination.
- **Received Datagrams With Unknown Protocol** — The number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol. This counter is incremented at the interface to which these datagrams were addressed which might not be necessarily the input interface for some of the datagrams.
- **Received Datagrams Discarded Due To Invalid Address** — The number of input datagrams discarded because the IPv6 address in their IPv6 header's destination field was not a valid address to be received at this entity. This count includes invalid addresses (for example, ::0) and unsupported addresses (for example, addresses with unallocated prefixes). For entities which are not IPv6 routers and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.
- **Received Datagrams Discarded Dut To Truncated Data** — The number of input datagrams discarded because datagram frame didn't carry enough data.
- **Received Datagrams Discarded Other** — The number of input IPv6 datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (for example, for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting re-assembly.
- **Received Datagrams Reassembly Required** — The number of IPv6 fragments received which needed to be reassembled at this interface. Note that this counter is incremented at the interface to which these fragments were addressed which might not be necessarily the input interface for some of the fragments.
- **Datagrams Successfully Reassembled** — The number of IPv6 datagrams successfully reassembled. Note that this counter is incremented at the interface to which these datagrams were addressed which might not be necessarily the input interface for some of the fragments.
- **Datagrams Failed To Reassemble** — The number of failures detected by the IPv6 reassembly algorithm (for whatever reason: timed out, errors, etc.). Note that this is not necessarily a count of discarded IPv6 fragments since some algorithms (notably the algorithm in RFC 815) can lose track of the number of fragments by combining them as they are received. This counter is incremented at the interface to which these fragments were addressed which might not be necessarily the input interface for some of the fragments.
- **Datagrams Forwarded** — The number of output datagrams which this entity received and forwarded to their final destinations. In entities which do not act as IPv6 routers, this counter includes only those packets which were Source-Routed through this entity, and the Source-Route processing was successful. Note that for a successfully forwarded datagram the counter of the outgoing interface is incremented.
- **Datagrams Locally Transmitted** — The number of datagrams which this entity has successfully transmitted from this output interface.

Downloaded from www.Manualslib.com manuals search engine

- **Datagrams Transmit Failed** — The number of datagrams which this entity failed to transmit successfully.
- **Datagrams Successfully Fragmented** — The number of IPv6 datagrams that have been successfully fragmented at this output interface.
- **Datagrams Failed To Fragment** — The number of output datagrams that could not be fragmented at this interface.
- **Datagrams Fragments Created** — The number of output datagram fragments that have been generated as a result of fragmentation at this output interface.
- **Multicast Datagrams Received** — The number of multicast packets received by the interface.
- **Multicast Datagrams Transmitted** — The number of multicast packets transmitted by the interface.

ICMPv6 Statistics

- **Total ICMPv6 Messages Received** — The total number of ICMP messages received by the interface which includes all those counted by ipv6IfIcmpInErrors. Note that this interface is the interface to which the ICMP messages were addressed which may not be necessarily the input interface for the messages.
- **ICMPv6 Messages With Errors Received** — The number of ICMP messages which the interface received but determined as having ICMP-specific errors (bad ICMP checksums, bad length, etc.)
- **ICMPv6 Destination Unreachable Messages Received** — The number of ICMP Destination Unreachable messages received by the interface.
- **ICMPv6 Messages Prohibited Administratively Received** — The number of ICMP destination unreachable/communication administratively prohibited messages received by the interface.
- **ICMPv6 Time Exceeded Messages Received** — The number of ICMP Time Exceeded messages received by the interface.
- **ICMPv6 Parameter Problem Messages Received** — The number of ICMP Parameter Problem messages received by the interface.
- **ICMPv6 Packet Too Big Messages Received** — The number of ICMP Packet Too Big messages received by the interface.
- **ICMPv6 Echo Request Messages Received** — The number of ICMP Echo (request) messages received by the interface.
- **ICMPv6 Echo Reply Messages Received** — The number of ICMP Echo Reply messages received by the interface.
- **ICMPv6 Router Solicit Messages Received** — The number of ICMP Router Solicit messages received by the interface.
- **ICMPv6 Router Advertisement Messages Received** — The number of ICMP Router Advertisement messages received by the interface.
- **ICMPv6 Neighbor Solicit Messages Received** — The number of ICMP Neighbor Solicit messages received by the interface.

Downloaded from www.Manualslib.com manuals search engine

- **ICMPv6 Neighbor Advertisement Messages Received** — The number of ICMP Neighbor Advertisement messages received by the interface.
- **ICMPv6 Redirect Messages Received** — The number of ICMPv6 Redirect messaged received by the interface.
- **ICMPv6 Group Membership Query Messages Received** — The number of ICMPv6 Group Membership Query messages received by the interface.
- **ICMPv6 Group Membership Response Messages Received** — The number of ICMPv6 Group Membership Response messages received by the interface.
- **ICMPv6 Group Membership Reduction Messages Received** — The number of ICMPv6 Group Membership Reduction messages received by the interface
- **Total ICMPv6 Messages Transmitted** — The total number of ICMP messages which this interface attempted to send. Note that this counter includes all those counted by icmpOutErrors.
- **ICMPv6 Messages Not Transmitted Due To Error** — The number of ICMP messages which this interface did not send due to problems discovered within ICMP such as a lack of buffers. This value should not include errors discovered outside the ICMP layer such as the inability of IPv6 to route the resultant datagram. In some implementations there may be no types of error which contribute to this counter's value.
- **ICMPv6 Destination Unreachable Messages Transmitted** — The number of ICMP Destination Unreachable Messages sent by the interface.
- **ICMPv6 Messages Prohibited Administratively Transmitted** — Number of ICMP destination unreachable/communication administratively prohibited messages sent.
- **ICMPv6 Time Exceeded Messages Transmitted** — The number of ICMP Time Exceeded messages sent by the interface.
- **ICMPv6 Parameter Problem Messages Transmitted** — The number of ICMP Parameter Problem messages sent by the interface.
- **ICMPv6 Packet Too Big Messages Transmitted** — The number of ICMP Packet Too Big messages sent by the interface.
- **ICMPv6 Echo Request Messages Transmitted** — The number of ICMP Echo (request) messages sent by the interface.
- **ICMPv6 Echo Reply Messages Transmitted** — The number of ICMP Echo Reply messages sent by the interface.
- **ICMPv6 Router Solicit Messages Transmitted** — The number of ICMP Router Solicitation messages sent by the interface.
- **ICMPv6 Router Advertisement Messages Transmitted** — The number of ICMP Router Advertisement messages sent by the interface.
- **ICMPv6 Neighbor Solicit Messages Transmitted** — The number of ICMP Neighbor Solicitation messages sent by the interface.

Downloaded from www.Manualslib.com manuals search engine

- **ICMPv6 Neighbor Advertisement Messages Transmitted** — The number of ICMP Neighbor Advertisement messages sent by the interface.
- **ICMPv6 Redirect Messages Transmitted** — The number of Redirect messages sent.
- **ICMPv6 Group Membership Query Messages Transmitted** — The number of ICMPv6 Group Membership Query messages sent.
- **ICMPv6 Group Membership Response Messages Transmitted** — The number of ICMPv6 Group Membership Response messages sent.
- **ICMPv6 Group Membership Reduction Messages Transmitted** — The number of ICMPv6 Group Membership Reduction messages sent.
- **ICMPv6 Duplicate Address Detects** — The number of duplicate Addressees detected by the interface.

Displaying IPv6 Statistics

1. Open the **IPv6 Statistics** page.
2. Select the interface to be displayed from the **Interface** drop-down menu.

   Statistics for the selected interface display.

Displaying IPv6 and ICMPv6 Statistics using the CLI Command

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- IPv6 Routing Commands

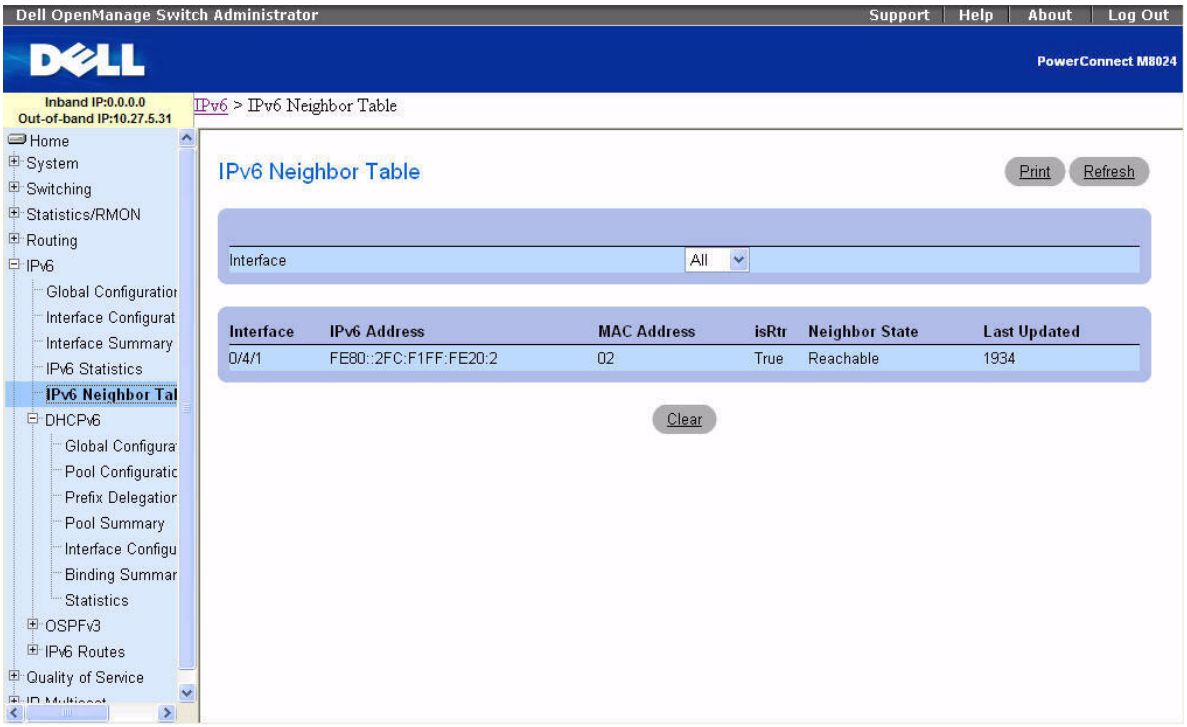
Downloaded from www.Manualslib.com manuals search engine

IPv6 Neighbor Table

Use the **IPv6 Neighbor Table** page to display IPv6 neighbor details for a specified interface.

To display the page, click **IPv6 > IPv6 Neighbor Table** in the tree view.

Figure 10-5. IPv6 Neighbor Table



The **IPv6 Neighbor Table** page contains the following fields:

- **Interface** — Selects the interface for which neighbor state information is displayed.
- **Interface** — Specifies the interface whose settings are displayed in the current table row.
- **IPv6 Address** — Specifies the IPv6 address of neighbor or interface.
- **MAC Address** — Specifies MAC address associated with an interface.
- **IsRtr** —Indicates whether the neighbor is a router. If the neighbor is a router, the value is TRUE. If the neighbor is not a router, the value is FALSE.
- **Neighbor State** — Specifies the state of the neighbor cache entry. Following are the states for dynamic entries in the IPv6 neighbor discovery cache:
  - **Incmp** — Address resolution is being performed on the entry. A neighbor solicitation message has been sent to the solicited-node multicast address of the target, but the corresponding neighbor advertisement message has not yet been received.

Downloaded from www.Manualslib.com manuals search engine

- **Reachable** — Positive confirmation was received within the last Reachable Time milliseconds that the forward path to the neighbor was functioning properly. While in REACH state, the device takes no special action as packets are sent.
- **Stale** — More than ReachableTime milliseconds have elapsed since the last positive confirmation was received that the forward path was functioning properly. While in STALE state, the device takes no action until a packet is sent.
- **Delay** — More than ReachableTime milliseconds have elapsed since the last positive confirmation was received that the forward path was functioning properly. A packet was sent within the last DELAY_FIRST_PROBE_TIME seconds. If no reachability confirmation is received within DELAY_FIRST_PROBE_TIME seconds of entering the DELAY state, send a neighbor solicitation message and change the state to PROBE.
- **Probe** — A reachability confirmation is actively sought by resending neighbor solicitation messages every RetransTimer milliseconds until a reachability confirmation is received.

- **Last Updated** — Time since the address was confirmed to be reachable.

Displaying IPv6 Neighbor Table

1. Open the **IPv6 Neighbor Table** page.
2. Select the interface to be displayed from the **Interface** drop-down menu.

   Neighbor details for the selected interface display.

Displaying IPv6 Neighbor Table using the CLI Command

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- IPv6 Routing Commands

DHCPv6

DHCP is generally used between clients (for example hosts) and servers (for example routers) for the purpose of assigning IP addresses, gateways, and other networking definitions such as DNS, NTP, and/or Session Initiation Protocol (SIP) parameters. However, IPv6 natively provides for auto configuration of IP addresses through IPv6 Neighbor Discovery Protocol (NDP) and the use of Router Advertisement messages. Thus, the role of DHCPv6 within the network is different than that of DHCPv4 in that it is less relied upon for IP address assignment.

There is a list of DHCP options that is commonly supported by DHCPv4 that need to be supported also by DHCPv6, and must be configured.

Note: The most important DHCP option to configure is the DNS Server option, which is configured on the **IPv6** → **DHCPv6** →**Pool Configuration** web page.

Downloaded from www.Manualslib.com manuals search engine

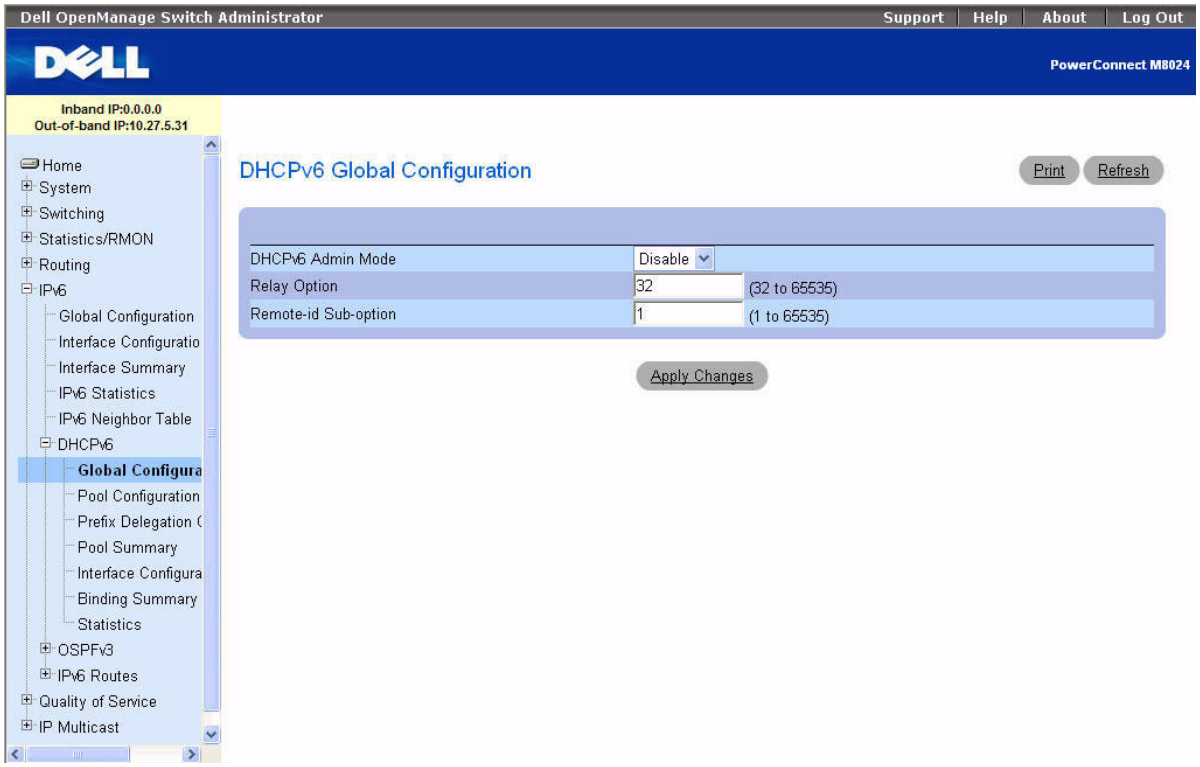
The **DHCPv6** menu page contains links to web pages that define and display DHCPv6 parameters and data. To display this page, click **IPv6 > DHCPv6** in the tree view. Following are the web pages accessible from this menu page:

- DHCPv6 Global Configuration
- DHCPv6 Pool Configuration
- Prefix Delegation Configuration
- DHCPv6 Pool Summary
- DHCPv6 Interface Configuration
- DHCPv6 Server Bindings Summary
- DHCPv6 Statistics

DHCPv6 Global Configuration

Use the **DHCPv6 Global Configuration** page to configure DHCPv6 global parameters. To display the page, click **IPv6 > DHCPv6 > Global Configuration** in the tree view.

Figure 10-6. DHCPv6 Global Configuration



Downloaded from www.Manualslib.com manuals search engine

The **DHCPv6 Global Configuration** page contains the following fields:

- **DHCPv6 Admin Mode** — Specifies DHCPv6 operation on the switch. Possible values are Enable and Disable; the default value is Disable.
- **Relay Option** — Specifies Relay Agent Information Option value. The values allowed are between 32 to 65535, and represent the value exchanged between the relay agent and the server. Each value has a different meaning, of which 1 to 39 are standardized. The default value, 32, means OPTION_INFORMATION_REFRESH_TIME.
- **Remote-id Sub-option** — Lets you specify a number to represent the Relay Agent Information Option Remote-ID Sub-option type. The values allowed are between 1 and 65535. The default value is 1.

Configuring DHCPv6 Global Parameters

1. Open the **DHCPv6 Global Configuration** page.
2. Modify the fields as needed.
3. Click **Apply Changes**.

   The DHCPv6 parameter modifications are saved, and the device is updated.

Configuring DHCPv6 Global Parameters using the CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- DHCPv6 Commands

Downloaded from www.Manualslib.com manuals search engine

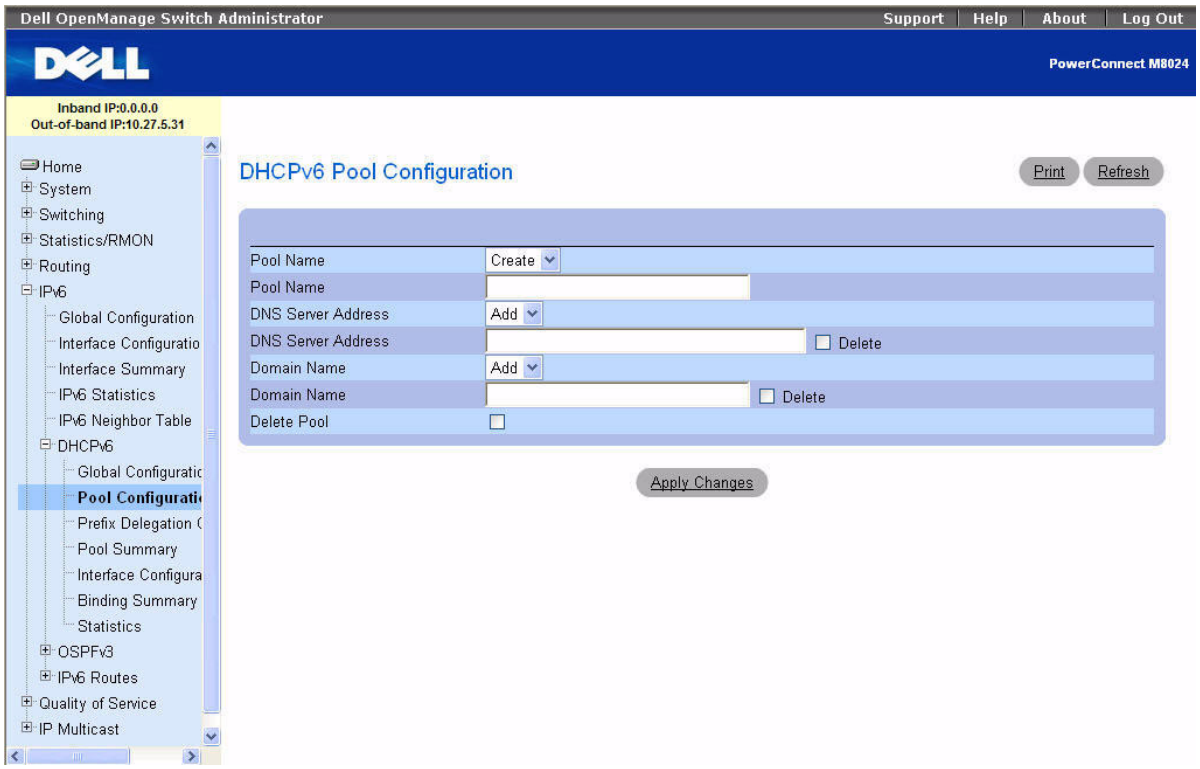
DHCPv6 Pool Configuration

DHCP for IPv6 clients are connected to a server which is configured to use parameters from a pool that you set up. The pool is identified with a pool name, and contains IPv6 addresses and domain names of DNS servers.

Use the **Pool Configuration** page to create a pool and/or configure pool parameters.

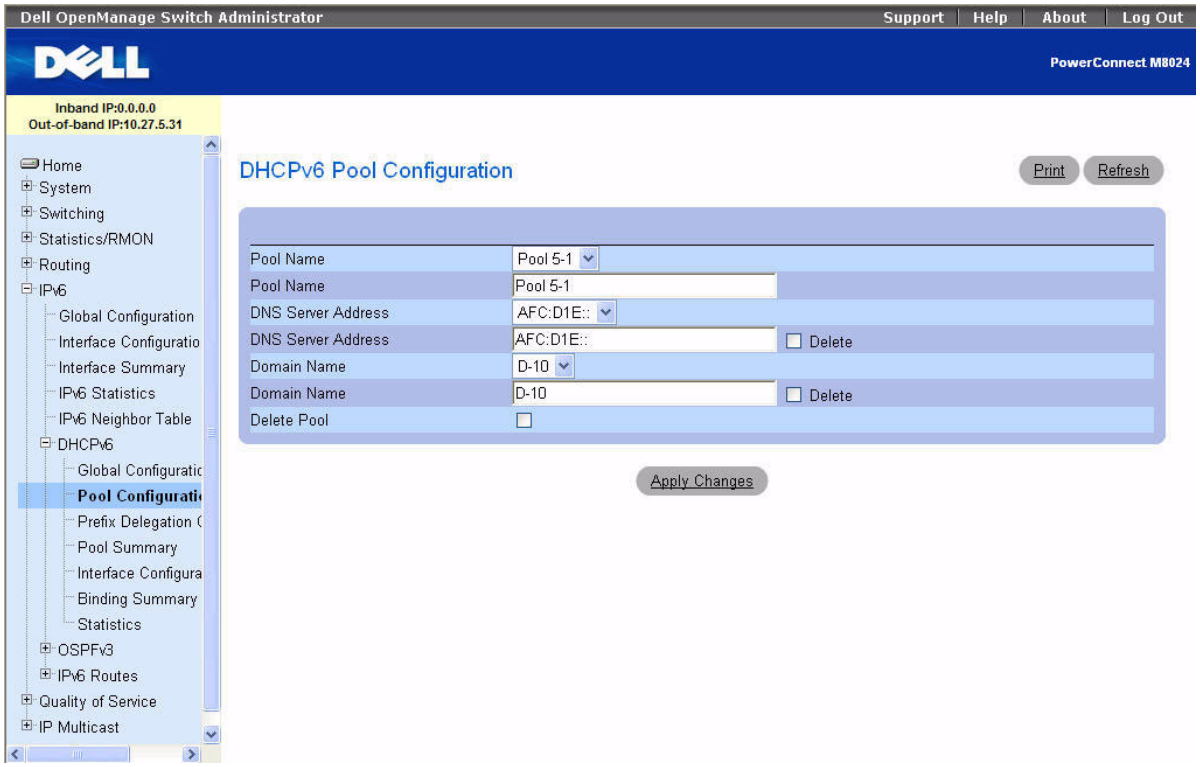
To display the page, click **IPv6 > DHCPv6 > Pool Configuration** in the tree view.

Figure 10-7. Pool Configuration - Create



Downloaded from www.Manualslib.com manuals search engine

Figure 10-8. Pool Configuration - Display



The **Pool Configuration** page contains the following fields:

- **Pool Name** — Drop-down menu that lists all the pool names configured. When **Create** is selected, fields on the page are cleared of data, in preparation for new pool information.
- **Pool Name** — Displays the pool selected from the previous field, or provides entry of a unique name for a DHCPv6 pool when Create is selected. A maximum of 31 alphanumeric characters can be entered.
- **DNS Server Address** — Drop-down menu that specifies the IPv6 address of a DNS server within a particular DHCPv6 pool. When **Add** is selected from the menu, the following field is cleared of data, in preparation for a new address.
- **DNS Server Address** — Displays the selected DNS server address from the previous field. Enter a new DNS server address here when Add is selected in the previous field. Click **Delete** to remove an address from this pool. The address is deleted when **Apply Changes** is clicked.
- **Domain Name** — Drop-down menu that specifies the list of domain names configured within a particular DHCPv6 pool. When **Add** is selected from the menu, the following field is cleared of data, in preparation for a new name.

Downloaded from www.Manualslib.com manuals search engine

- **Domain Name** — Displays the selected DNS domain name from the previous field. Enter a new DNS domain name here when Add is selected in the previous field. A maximum of 255 alphanumeric characters can be entered. Click **Delete** to remove a domain name from this pool. The name is deleted when **Apply Changes** is clicked.
- **Delete Pool** — Check this box to delete the displayed pool. The pool is deleted when **Apply Changes** is clicked.

Creating a DHCPv6 Pool

1. Open the **Pool Configuration** page.
2. Select Create from the Pool Name drop-down menu.
3. Enter a new name in the Pool Name field.
4. Specify an existing DNS Server Address to associate with this pool, or create a new one.
5. Specify an existing Domain Name to associate with this pool, or create a new one.
6. Click **Apply Changes**.

   The new pool is saved, and the device is updated. If a new DNS server address or domain name was specified, it is also saved.

Modifying DHCPv6 Pool Parameters

1. Open the **Pool Configuration** page.
2. Select the pool for which parameters are changing from the drop-down Pool Name menu.
3. Change or set up a new DNS Server Address for the specified pool.
4. Change or set up a new Domain Name for the specified pool.
5. Click **Apply Changes**.

   The DHCPv6 Pool parameter modifications are saved, and the device is updated.

Deleting a DHCPv6 Pool or Parameter

1. Open the **Pool Configuration** page.
2. Select the pool to be affected from the drop-down Pool Name menu.
3. Click the Delete box if deleting the DNS Server Address for this pool.
4. Click the Delete box if deleting the Domain Name for this pool.
5. Click the Delete Pool box if deleting the entire pool.
6. Click **Apply Changes**.

   The pool or its parameter setting is deleted, and the device is updated.

Downloaded from www.Manualslib.com manuals search engine

Configuring DHCPv6 Pool Parameters using the CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

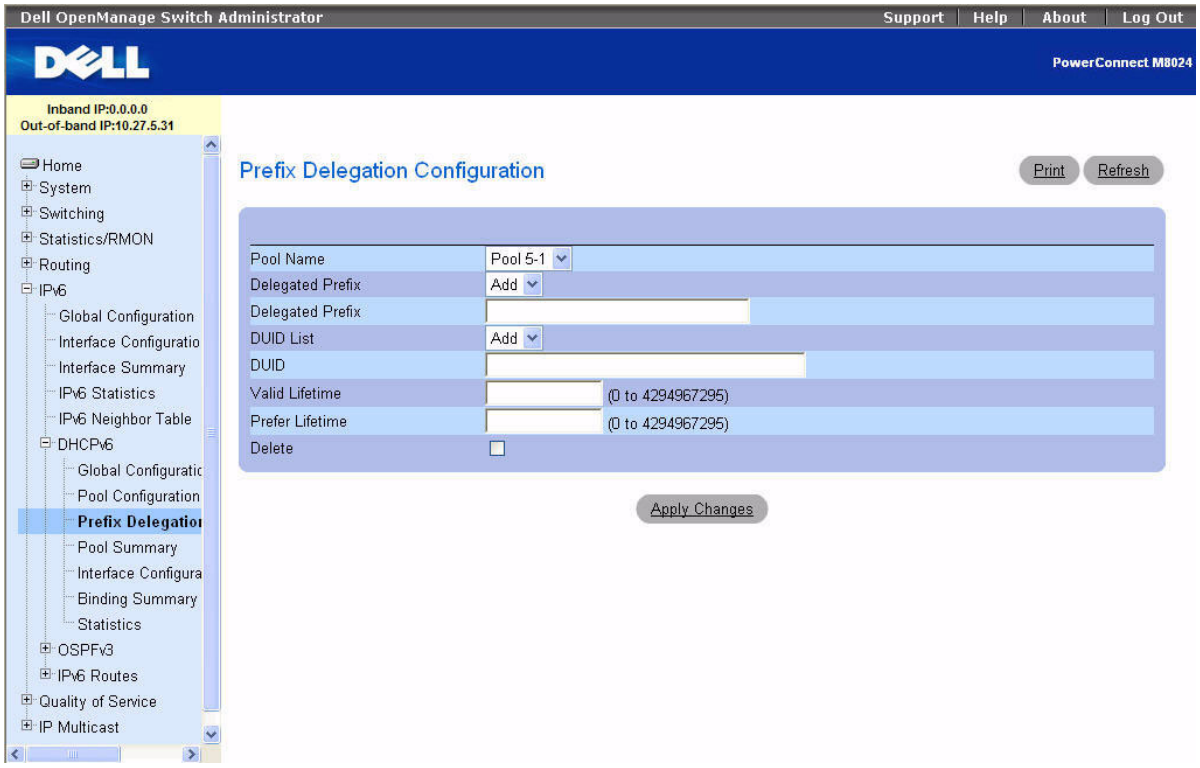
- DHCPv6 Commands

Prefix Delegation Configuration

Use the **Prefix Delegation Configuration** page to configure a delegated prefix for a pool. At least one pool must be created using DHCPv6 Pool Configuration before a delegated prefix can be configured.

To display the page, click **IPv6 > DHCPv6 > Prefix Delegation Configuration** in the tree view.

Figure 10-9. Prefix Delegation Configuration



The **Prefix Delegation Configuration** page contains the following fields:

- **Pool Name** — Specifies all the pool names configured. Select the pool to configure.
- **Delegated Prefix** — Drop-down menu that specifies the delegated IPv6 prefix to associate with the specified pool. Select **Add** to define a new delegated prefix for this pool.
- **Delegated Prefix** — Displays selected delegated prefix or allows entry of new one.
- **DUID List** - Drop-down menu that selects the client's unique DUID value. Select **Add** to define a new DUID value for this pool.

Downloaded from www.Manualslib.com manuals search engine

- **DUID** - Displays selected DUID value or allows entry of new one.
- **Valid Lifetime** — Specifies the valid lifetime in seconds for delegated prefix.
- **Prefer Lifetime** — Specifies the prefer lifetime in seconds for delegated prefix.
- **Delete** — Deletes the displayed pool prefix delegation configuration when checked and **Apply Changes** is clicked.

Configuring a delegated prefix to a Pool

1. Open the **Prefix Delegation Configuration** page.
2. Select the pool to be configured.
3. Specify the delegated prefix.
4. Modify the remaining fields as needed.
5. Click **Apply Changes**.

   The delegated prefix and parameters are saved, and the device is updated.

Configuring a delegated prefix using the CLI Command

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- DHCPv6 Commands

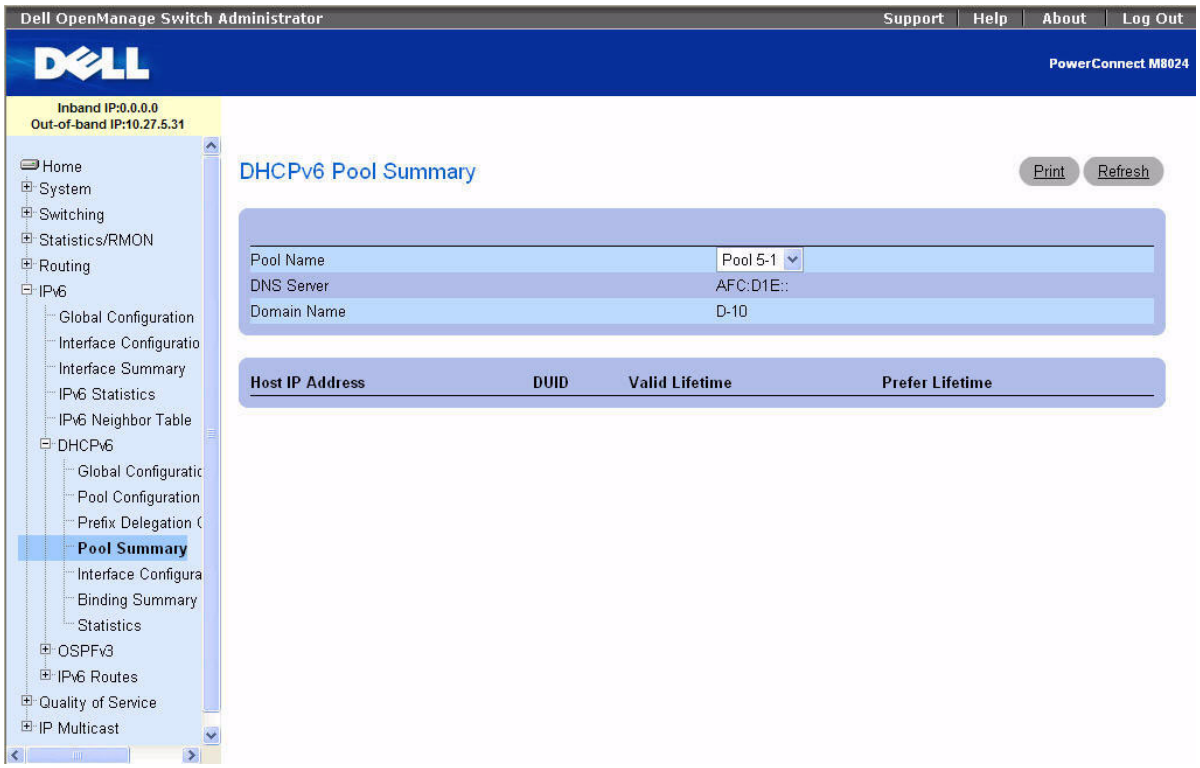
Downloaded from www.Manualslib.com manuals search engine

DHCPv6 Pool Summary

Use the **Pool Summary** page to display settings for all DHCPv6 Pools. At least one pool must be created using DHCPv6 Pool Configuration before the Pool Summary displays.

To display the page, click **IPv6 > DHCPv6 > Pool Summary** in the tree view.

Figure 10-10. Pool Summary



The **Pool Summary** page contains the following fields:

- **Pool Name** — Selects the pool to display.
- **DNS Server** — Displays the IPv6 address of the associated DNS server.
- **Domain Name** — Displays the DNS domain name.
- **Host IP Address** — Displays the IPv6 address and mask length for the delegated prefix.
- **DUID** — Identifier used to identify the client's unique DUID value.
- **Valid Lifetime** — Displays the valid lifetime in seconds for delegated prefix.
- **Prefer Lifetime** — Displays the preferred lifetime in seconds for delegated prefix.

Downloaded from www.Manualslib.com manuals search engine

Displaying the Pool Summary using the CLI Command

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

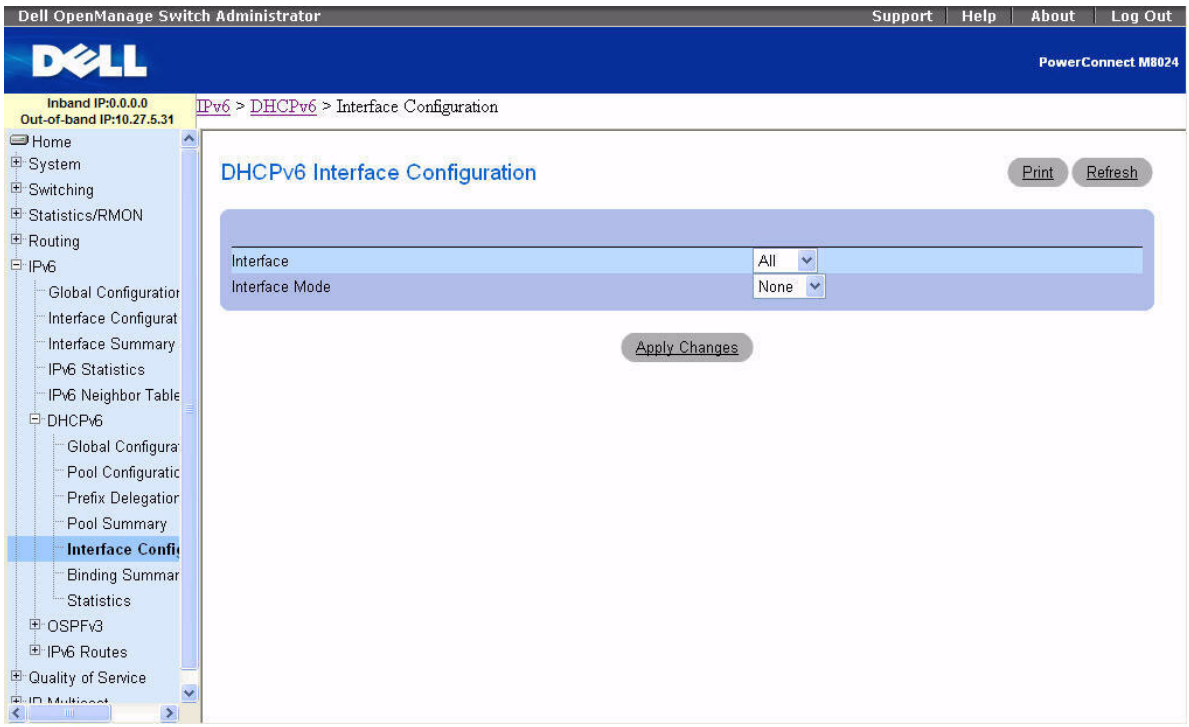
- DHCPv6 Commands

DHCPv6 Interface Configuration

Use the **DHCPv6 Interface Configuration** page to configure a DHCPv6 interface.

To display the page, click **IPv6 > DHCPv6 > Interface Configuration** in the tree view.

Figure 10-11. DHCPv6 Interface Configuration



The **DHCPv6 Interface Configuration** pages contain the following fields:

Interface — Select the interface for which you are configuring DHCPv6 server functionality.

Interface Mode — Configure the DHCPv6 mode as either Server or Relay. DHCPv6 server and DHCPv6 relay functions are mutually exclusive.

Pool Name — Selects the DHCPv6 pool containing stateless and/or prefix delegation parameters. This field displays when the Interface Mode is Server.

Rapid Commit — Rapid commit is an optional parameter. Specified to allow abbreviated exchange between the client and server. This field displays when the Interface Mode is Server.

Preference — Selects the preference value used by clients to determine preference between multiple DHCPv6 servers. The values allowed are between 0 to 4294967295. This field displays when the Interface Mode is Server.

Downloaded from www.Manualslib.com manuals search engine

Delete — Check this box and click **Apply Changes** to delete this configuration. This field displays when the Interface Mode is Server or Relay.

Relay Interface — Selects the interface to reach a relay server. This field displays when the Interface Mode is Relay.

Destination IP Address — Selects the IPv6 address of the DHCPv6 relay server. This field displays when the Interface Mode is Relay.

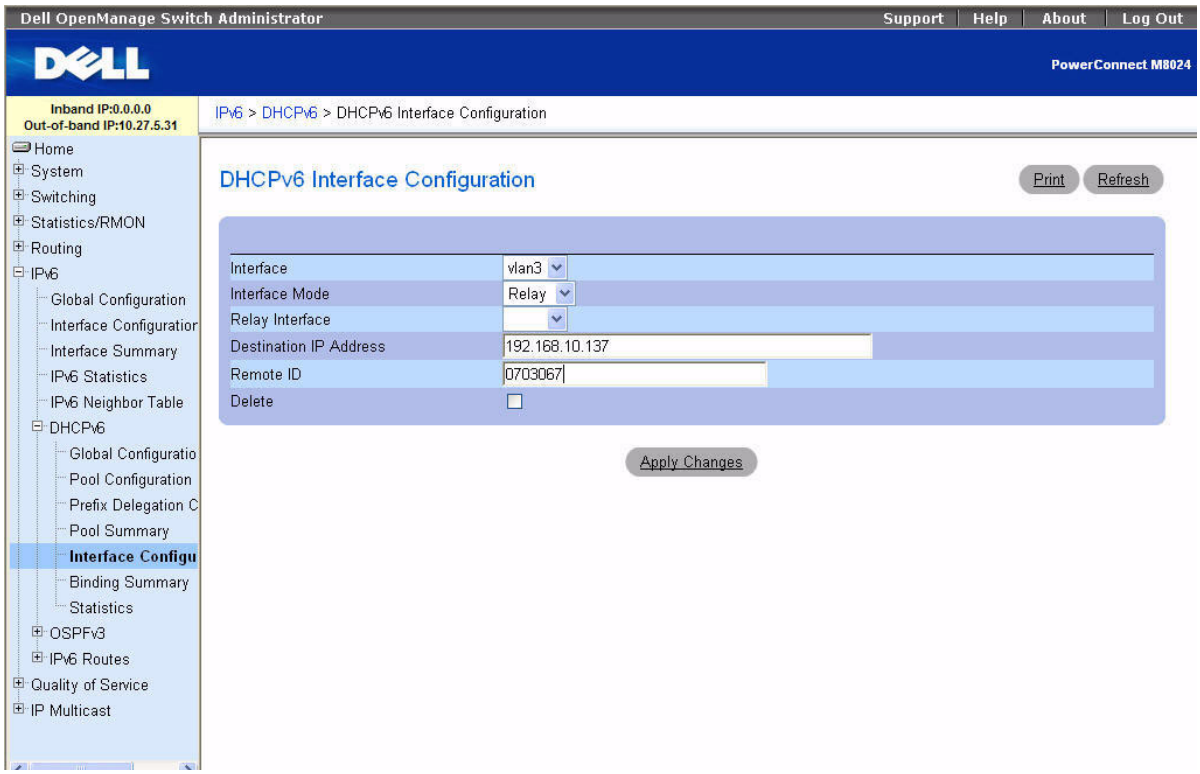
Remote ID — Selects the relay agent information option. the Remote ID needs to be derived from the DHCPv6 server DUID and the relay interface number, or it can be specified as a user-defined string. This field displays when the Interface Mode is Relay.

Configuring a DHCPv6 Interface for Relay Interface Mode

1. Open the **DHCPv6 Interface Configuration** page.
2. Specify the desired Interface, and select **Relay** from the **Interface Mode** drop down menu.

   The following screen appears:

Figure 10-12. DHCPv6 Interface Configuration - Relay



3. Modify the fields as needed.
4. Click **Apply Changes**.

   The DHCPv6 interface configuration is saved, and the device is updated.

Downloaded from www.Manualslib.com manuals search engine

Configuring a DHCPv6 Interface Using the CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

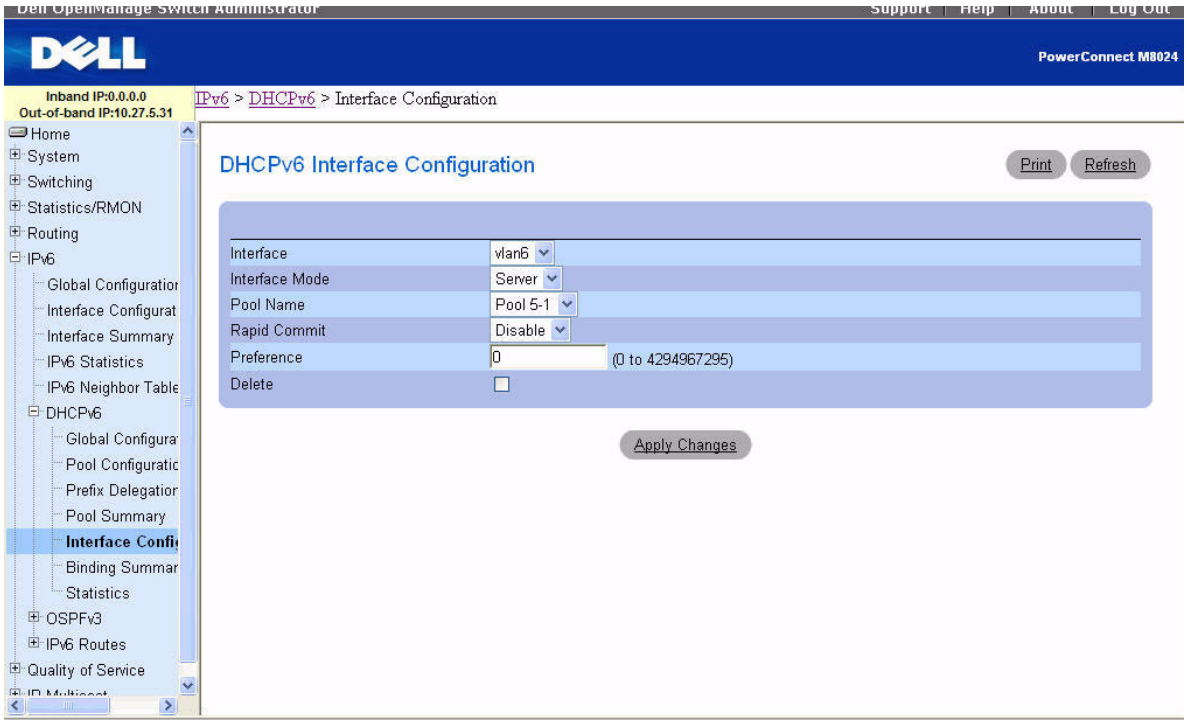
- DHCPv6 Commands

Configuring a DHCPv6 Interface for Server Interface Mode

1. Open the **DHCPv6 Interface Configuration** page.
2. Specify the desired Interface, and select **Server** from the **Interface Mode** drop down menu.

   The following screen appears:

Figure 10-13. DHCPv6 Interface Configuration - Server



3. Modify the fields as needed.
4. Click **Apply Changes**.

   The DHCPv6 interface configuration is saved, and the device is updated.

Downloaded from www.Manualslib.com manuals search engine

Configuring a DHCPv6 Interface for Server Interface Mode Using the CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

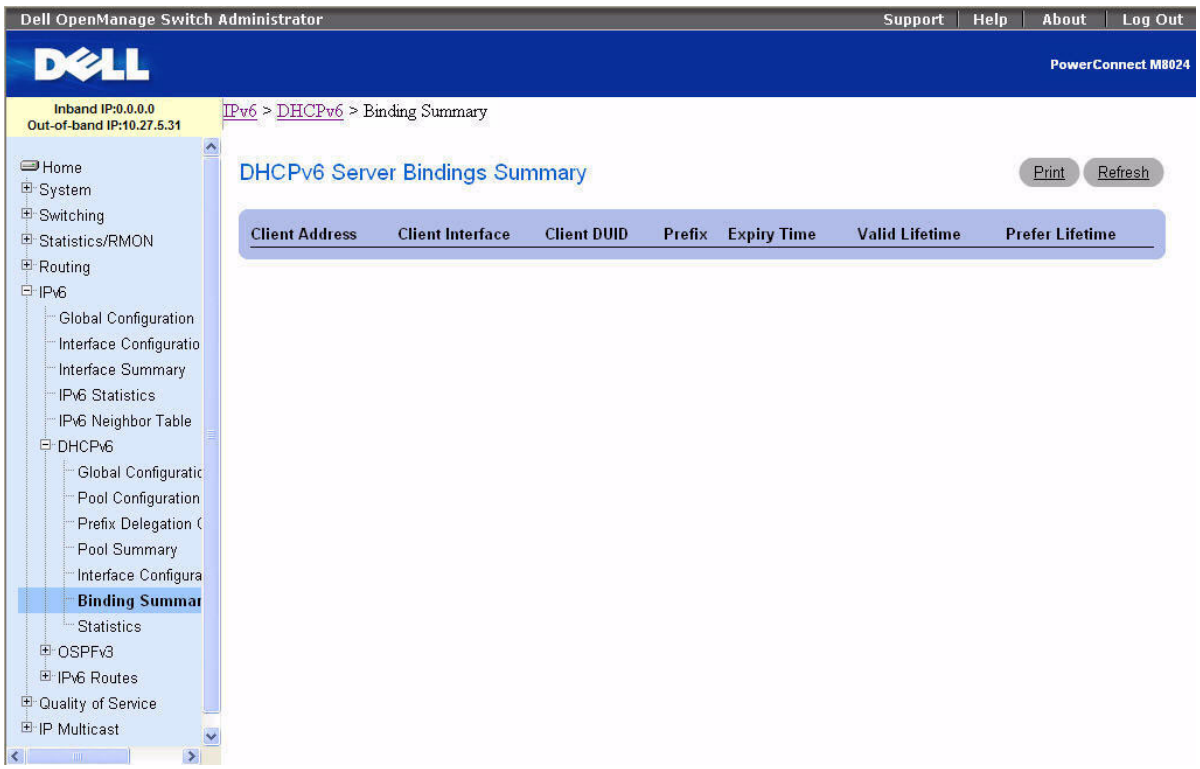
- DHCPv6 Commands

DHCPv6 Server Bindings Summary

Use the **Server Bindings Summary** page to display all DHCPv6 server bindings.

To display the page, click **IPv6 > DHCPv6 > Bindings Summary** in the tree view.

Figure 10-14. Server Bindings Summary



The **Server Bindings Summary** page contains the following fields:

- **Client Address** — Specifies the IPv6 address of the client associated with the binding.
- **Client Interface** — Specifies the interface number where the client binding occurred.
- **Client DUID** — Specifies client's DHCPv6 unique identifier.
- **Prefix** - Specifies the type of prefix associated with this binding.
- **Expiry Time** — Specifies the number of seconds until the prefix associated with a binding expires.
- **Valid Lifetime** — Specifies the valid lifetime value in seconds of the prefix associated with a binding.

Downloaded from www.Manualslib.com manuals search engine

- **Prefer Lifetime** — Specifies the preferred lifetime value in seconds of the prefix associated with a binding.

Displaying Server Bindings using the CLI Command

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

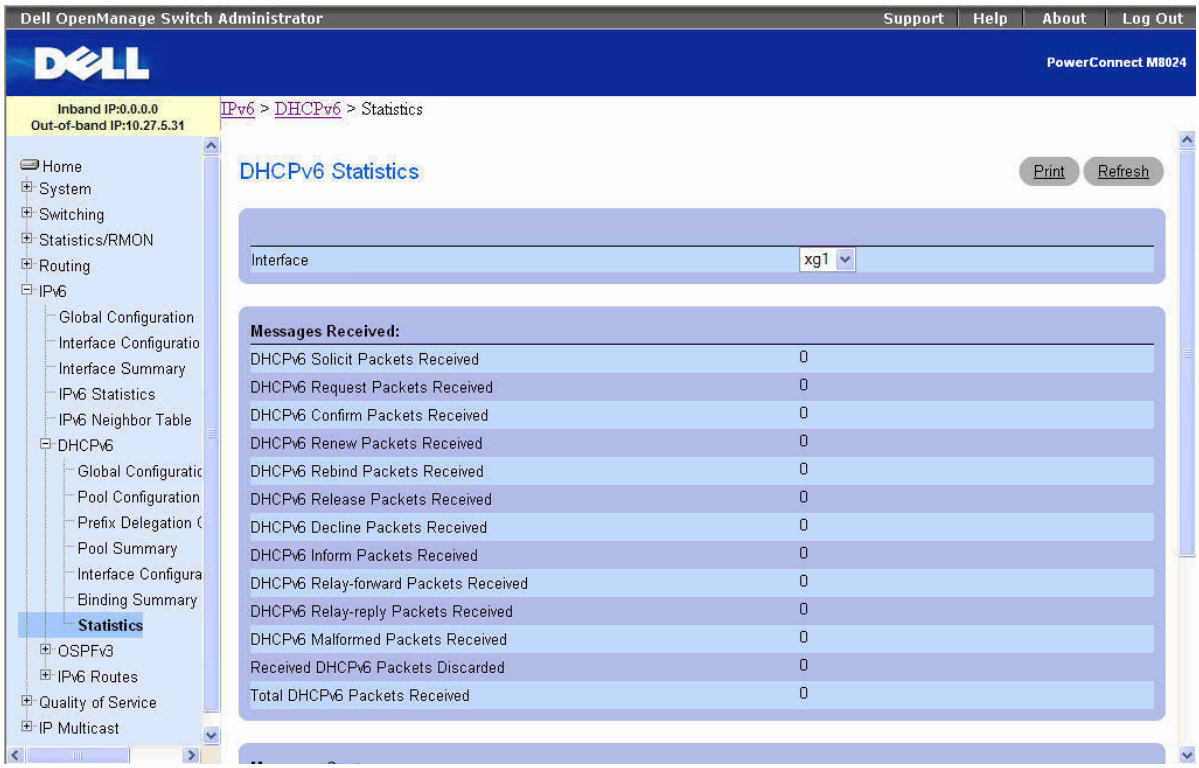
- DHCPv6 Commands

DHCPv6 Statistics

Use the **DHCPv6 Statistics** page to display DHCPv6 statistics for one or all interfaces.

To display the page, click **IPv6 > DHCPv6 > Statistics** in the tree view.

Figure 10-15. DHCPv6 Statistics



Downloaded from www.Manualslib.com manuals search engine

The **DHCPv6 Statistics** page displays the following fields:

- **Interface** — Select the interface for which data is to be displayed or configured. On selecting **All**, data is shown for all interfaces.

Messages Received

This section specifies the aggregate of all interface level statistics for received messages:

- **DHCPv6 Solicit Packets Received** — Specifies the number of Solicits.
- **DHCPv6 Request Packets Received** — Specifies the number of Requests.
- **DHCPv6 Confirm Packets Received** — Specifies the number of Confirms.
- **DHCPv6 Renew Packets Received** — Specifies the number of Renews.
- **DHCPv6 Rebind Packets Received** — Specifies the number of Rebinds.
- **DHCPv6 Release Packets Received** — Specifies the number of Releases.
- **DHCPv6 Decline Packets Received** — Specifies the number of Declines.
- **DHCPv6 Inform Packets Received** — Specifies the number of Informs.
- **DHCPv6 Relay-forward Packets Received** — Specifies the number of Relay forwards.
- **DHCPv6 Relay-reply Packets Received** — Specifies the number of Relay Replies.
- **DHCPv6 Malformed Packets Received** — Specifies the number of Malformed Packets.
- **Received DHCPv6 Packets Discarded** — Specifies the number of Packets Discarded.
- **Total DHCPv6 Packets Received** — Specifies the total number of Packets Received.

Messages Sent

This section specifies the aggregate of all interface level statistics for messages sent:

- **DHCPv6 Advertisement Packets Transmitted** — Specifies the number of Advertisements.
- **DHCPv6 Reply Packets Transmitted** — Specifies the number of Replies.
- **DHCPv6 Reconfig Packets Transmitted** — Specifies the number of Reconfigurations.
- **DHCPv6 Relay-forward Packets Transmitted** — Specifies the number of Relay forwards.
- **DHCPv6 Relay-reply Packets Transmitted** — Specifies the number of Relay Replies.
- **Total DHCPv6 Packets Sent** — Specifies the total number of Packets Transmitted.
- **Clear** — Resets the interface packet counters.

Displaying DHCPv6 Statistics

1. Open the **DHCPv6 Statistics** page.
2. Select the interface to be displayed from the Interface drop-down menu.

   DHCPv6 statistics display for the selected interface.

Downloaded from www.Manualslib.com manuals search engine

Displaying DHCPv6 Statistics using the CLI Command

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- DHCPv6 Commands

OSPFv3

OSPFv3 is the Open Shortest Path First routing protocol for IPv6. It is similar to OSPFv2 in its concept of a link state database, intra/inter area, and AS external routes and virtual links. It differs from its IPv4 counterpoint in a number of respects, including the following: peering is done through link-local addresses; the protocol is link rather than network centric; and addressing semantics have been moved to leaf LSAs, which eventually allow its use for both IPv4 and IPv6. Point to point links are also supported in order to enable operation over tunnels.

It is possible to enable OSPF and OSPFv3 at the same time. OSPF works with IPv4 and OSPFv3 works with IPv6.

The **OSPFv3** menu page contains links to web pages that define and display OSPFv3 parameters and data. To display this page, click **IPv6 > OSPFv3** in the tree view.

Following are the web pages accessible from this menu page:

- OSPFv3 Configuration
- OSPFv3 Area Configuration
- OSPFv3 Stub Area Summary
- OSPFv3 Area Range Configuration
- OSPFv3 Interface Configuration
- OSPFv3 Interface Statistics
- OSPFv3 Neighbors
- OSPFv3 Neighbor Table
- OSPFv3 Link State Database
- OSPFv3 Virtual Link Configuration
- OSPFv3 Virtual Link Summary
- OSPFv3 Route Redistribution Configuration
- OSPFv3 Route Redistribution Summary

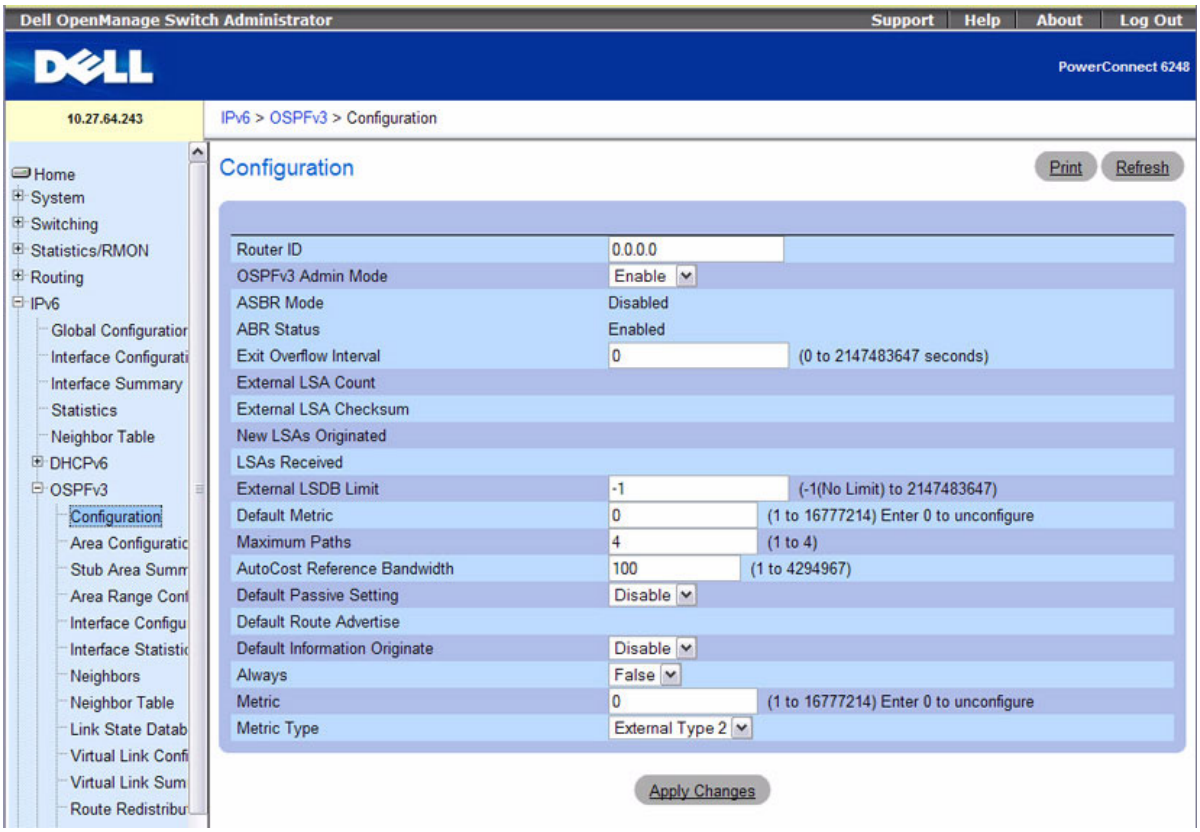
Downloaded from www.Manualslib.com manuals search engine

OSPFv3 Configuration

Use the **OSPFv3 Configuration** page to activate and configure OSPFv3 for a switch.

To display the page, click **IPv6 > OSPFv3 > Configuration** in the tree view.

Figure 10-16. OSPFv3 Configuration



The **OSPFv3 Configuration** page contains the following fields:

- **Router ID** — The 32-bit integer in dotted decimal format that uniquely identifies the router within the autonomous system (AS). If you want to change the Router ID you must first disable OSPFv3. After you set the new Router ID, you must re-enable OSPFv3 to have the change take effect. The default value is 0.0.0.0, although this is not a valid Router ID, and must be changed before you press the **Apply Changes** button.
- **OSPFv3 Admin Mode** — Select Enable or Disable from the drop-down menu. If you select Enable, OSPFv3 is activated for the switch. The default value is Enable. You must configure a Router ID before OSPFv3 becomes operational. This can also be done by issuing the CLI command, `router-id`, in the IPv6 router OSPF mode.

NOTE: Once OSPFv3 is initialized on the router, it remains initialized until the router is reset.

Downloaded from www.Manualslib.com manuals search engine

- **ASBR Mode** — Reflects whether the ASBR mode is enabled or disabled. Enable implies that the router is an autonomous system border router. Router automatically becomes an ASBR when it is configured to redistribute routes learned from other protocol.
- **ABR Status** — The values of this are Enable or Disable. The field displays only when a valid configuration exists. Enabled implies that the router is an area border router. Disabled implies that it is not an area border router.
- **Exit Overflow Interval** — Enter the number of seconds that, after entering overflow state, the router should wait before attempting to leave overflow state. This allows the router to again originate non-default AS-external-LSAs. If you enter 0, the router does not leave Overflow State until restarted. The range is 0 to 2147483647 seconds.
- **External LSA Count** — The number of external (LS type 5) LSAs (link state advertisements) in the link state database.
- **External LSA Checksum** — The sum of the LS checksums of the external LSAs (link state advertisements) contained in the link-state database. This sum can be used to determine if there has been a change in a router's link state database, and to compare the link-state databases of two routers.
- **New LSAs Originated** — In any given OSPFv3 area, a router originates several LSAs. Each router originates a router-LSA. If the router is also the Designated Router for any of the area's networks, it originates network-LSAs for those networks. This value represents the number of LSAs originated by this router.
- **LSAs Received** — The number of LSAs (link state advertisements) received that were determined to be new instantiations. This number does not include newer instantiations of self-originated LSAs.
- **External LSDB Limit** — The maximum number of AS-External-LSAs that can be stored in the database. A value of -1 implies there is no limit on the number that can be saved. The valid range of values is -1 to 2147483647.
- **Default Metric** — Sets a default for the metric of redistributed routes. This field displays the default metric if one has already been set or blank if not configured earlier. Valid values are 1 to 16777214.
- **Maximum Paths** — Configure the maximum number of paths that OSPFv3 can report to a given destination. Valid values are 1 to 4.
- **AutoCost Reference Bandwidth** — This field configures the value that OSPFv3 uses in calculating the default metric for an interface. OSPF calculates the link cost of each interface as:

  Cost = (Reference Bandwidth in Mbps) / (Interface Bandwidth).

  For example, setting this value to 1000 Mbps would cause all 1-Gbps interfaces to have a default cost of 1000/1000 = 1. For 100 Mbps interfaces, the default cost would be 1000/100 = 10.
- **Default Passive Setting** — Select whether OSPFv3 interfaces default to passive mode. In passive mode, interfaces do not send OSPF routing updates. This setting is disabled by default, so that all interfaces default to non-passive mode. If enabled, then all interfaces default to passive mode, and the network manager can selectively enable interfaces to send OSPF routing updates.

Downloaded from www.Manualslib.com manuals search engine

- **Default Route Advertise:** Use this section to configure the parameters for Default Route Advertisements into OSPF domain.
- **Default Information Originate** — Enable or disable Default Route Advertise.

NOTE: The values for Always, Metric, and Metric Type can only be configured after Default Information Originate is set to Enable.

If Default Information Originate is set to Enable and values for Always, Metric, and Metric Type are already configured, then setting Default Information Originate back to disable sets the Always, Metric, and Metric Type values to default.

- **Always** — Sets the router advertise ::/0 when set to True.
- **Metric** — Specifies the metric of the default route. Valid values are 0 to 16777214.

Metric Type — Sets the metric type of the default route. Valid values are External Type 1 and External Type 2.

Configuring OSPFv3

1. Open the **OSPFv3 Configuration** page.
2. Modify the fields as needed.
3. Click **Apply Changes**.

   The OSPFv3 configuration is saved, and the device is updated.

Configuring OSPFv3 using the CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- OSPFv3 Commands

Downloaded from www.Manualslib.com manuals search engine

OSPFv3 Area Configuration

Use the **OSPFv3 Area Configuration** page to create and configure an OSPFv3 area.

To display the page, click **IPv6 > OSPFv3 > Area Configuration** in the tree view.

Figure 10-17. OSPFv3 Area Configuration

The **OSPFv3 Area Configuration** page contains the following fields:

- **Area ID** — The OSPFv3 area. An Area ID is a 32-bit integer in dotted decimal format that uniquely identifies the area to which a router interface connects.
- **External Routing** — A definition of the router's capabilities for the area, including whether or not AS-external-LSAs are flooded into/throughout the area. If the area is a stub area, then these are the possible options for which you may configure the external routing capability, otherwise the only option is Import External LSAs.
- **SPF Runs** — The number of times that the intra-area route table has been calculated using this area's link-state database. This is typically done using Dijkstra's algorithm.
- **Area Border Router Count** — The total number of area border routers reachable within this area. This is initially zero, and is calculated in each SPF Pass.
- **Area LSA Count** — The total number of link-state advertisements in this area's link-state database, excluding AS External LSAs.

Downloaded from www.Manualslib.com manuals search engine

- **Area LSA Checksum** — The 32-bit unsigned sum of the link-state advertisements' LS checksums contained in this area's link-state database. This sum excludes external (LS type 5) link-state advertisements. The sum can be used to determine if there has been a change in a router's link state database, and to compare the link-state database of two routers. This value is in hexadecimal.

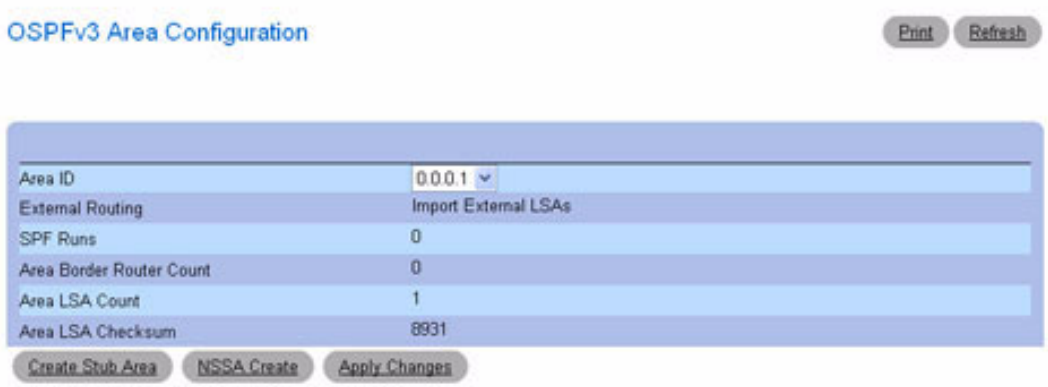
Configuring OSPFv3 Area

1. Open the **OSPFv3 Area Configuration** page.
2. Modify the fields as needed.
3. Click **Apply Changes**.

   The configuration is saved and the device is updated.

   The web page reappears with **Create Stub Area** and **NSSA Create** buttons.

Figure 10-18. OSPFv3 Area Configuration - Create Stub Area and NSSA Create



Configuring OSPFv3 Stub Area

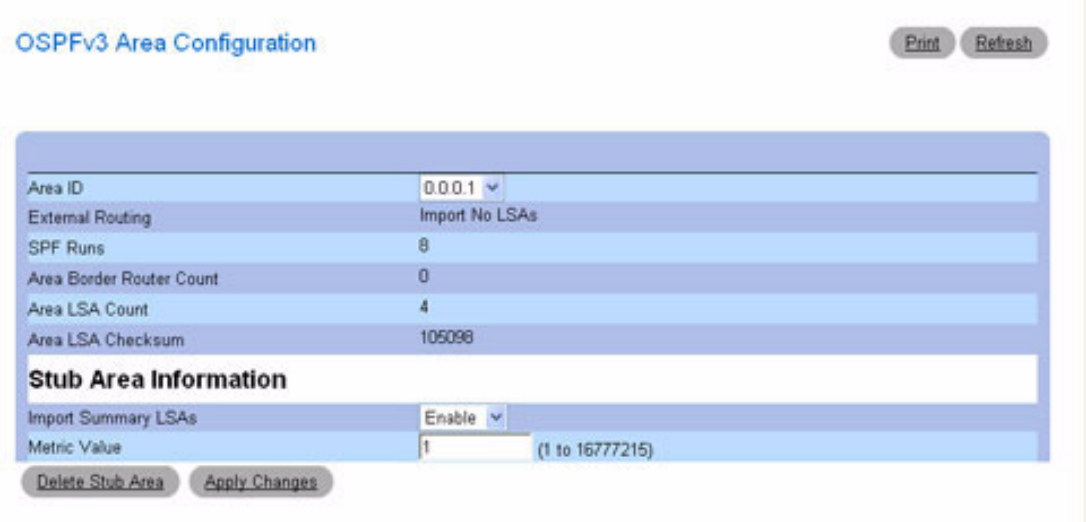
1. Open the **OSPFv3 Area Configuration** page.
2. Modify the fields as needed.
3. Click **Apply Changes**.

   The web page reappears with **Create Stub Area** and **NSSA Create** buttons. See Figure 10-18.
4. Click **Create Stub Area.**

   The **Stub Area Information** fields display.

Downloaded from www.Manualslib.com manuals search engine

Figure 10-19. OSPFv3 Stub Area Configuration



5. Complete the remaining fields.
6. Click **Apply Changes**.

   The Stub Area information is saved and the device is updated.

Configuring OSPFv3 NSSA Area

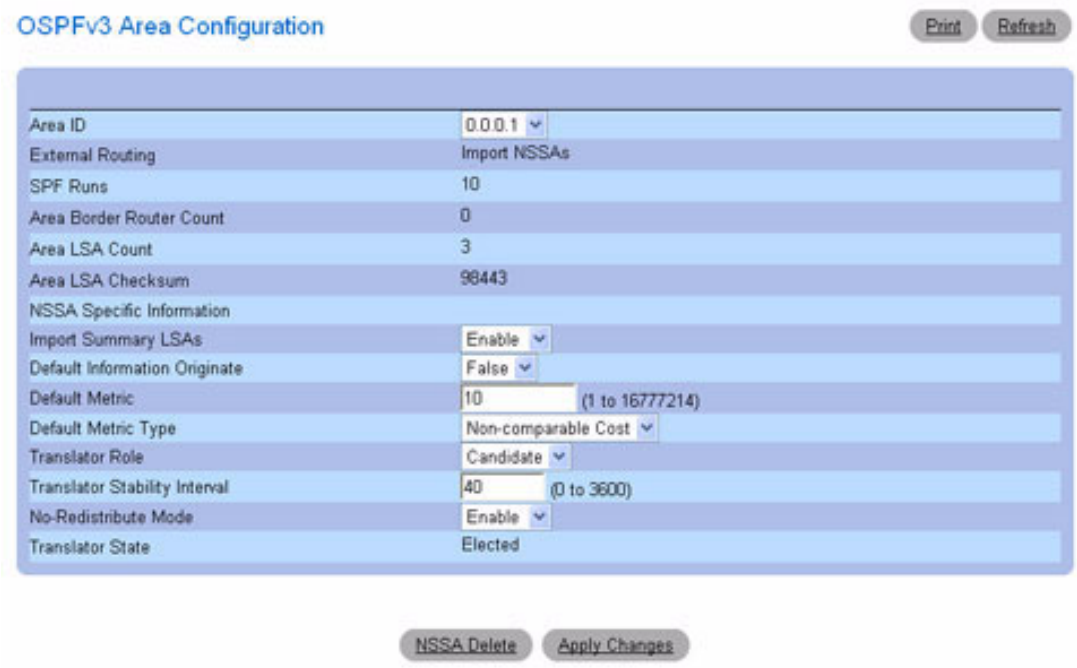
1. Open the **OSPFv3 Area Configuration** page.
2. Modify the fields as needed.
3. Click **Apply Changes**.

   The web page reappears with **Create Stub Area** and **NSSA Create** buttons. See Figure 10-18.
4. Click **NSSA Create** on the **OSPFv3 Area Configuration** web page.

   The web page reappears showing options for NSSA configuration.

Downloaded from www.Manualslib.com manuals search engine

Figure 10-20. OSPFv3 Area Configuration - NSSA



5. Complete the remaining fields.
6. Click **Apply Changes**.

   The NSSA information is saved and the device is updated.

Deleting OSPFv3 Stub Area Information

1. Open the **OSPFv3 Area Configuration** page with configured Stub Area information.
2. Click **Delete Stub Area**.
3. Click **Apply Changes**.

Deleting OSPFv3 NSSA Information

1. Open the **OSPFv3 Area Configuration** page with configured NSSA information.
2. Click **NSSA Delete**.
3. Click **Apply Changes**.

Configuring OSPFv3 Area using the CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- OSPFv3 Commands

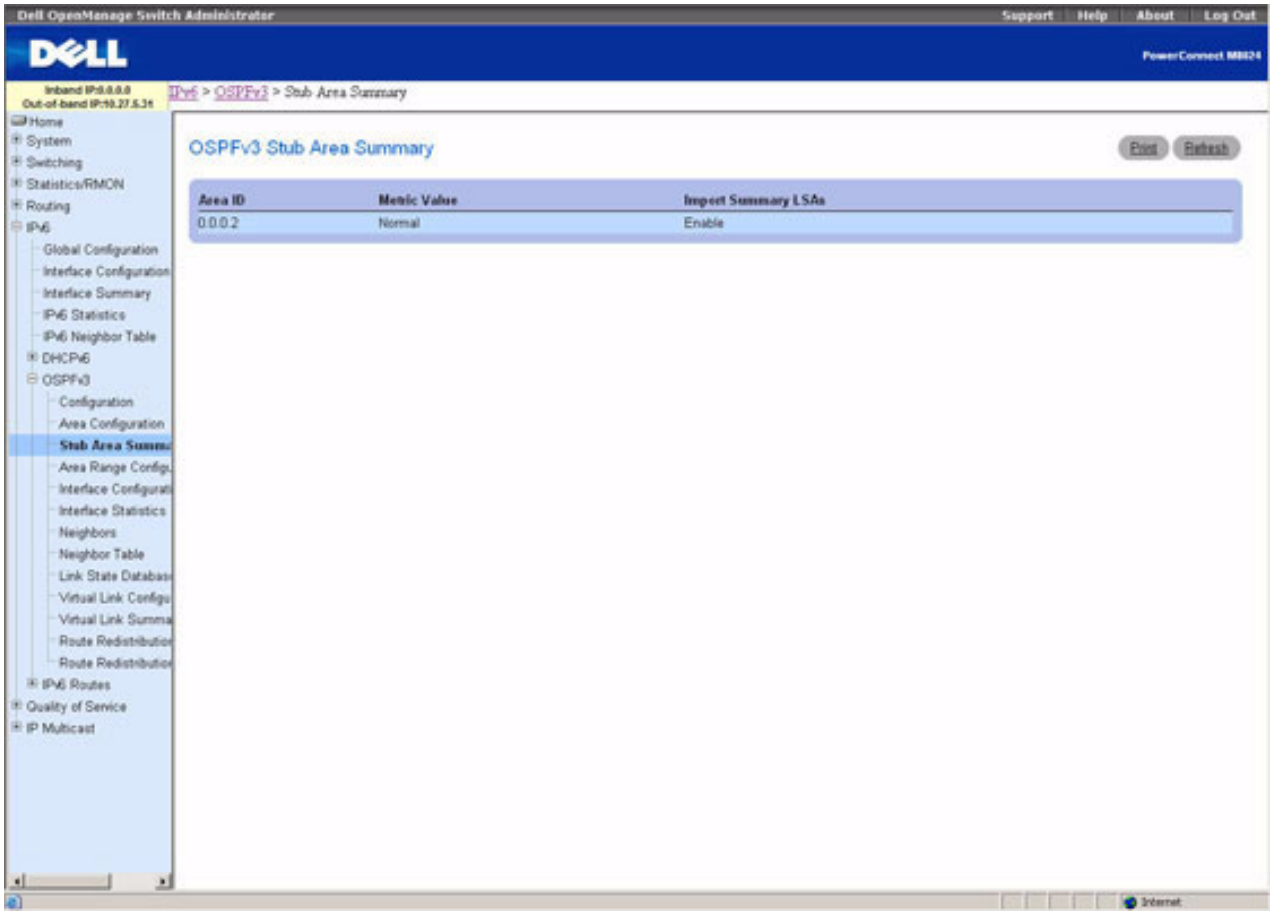
Downloaded from www.Manualslib.com manuals search engine

OSPFv3 Stub Area Summary

Use the **OSPFv3 Stub Area Summary** page to display OSPFv3 stub area detail.

To display the page, click **IPv6 > OSPFv3 > Stub Area Summary** in the tree view.

Figure 10-21. OSPFv3 Stub Area Summary



The **OSPFv3 Stub Area Summary** page displays the following fields:

- **Area ID** — The Area ID of the Stub area.
- **Metric Value** — The metric value applied to the default route advertised into the area.
- **Import Summary LSAs** — Whether the import of Summary LSAs is enabled or disabled.

Displaying the OSPFv3 Stub Area Summary using the CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- OSPFv3 Commands

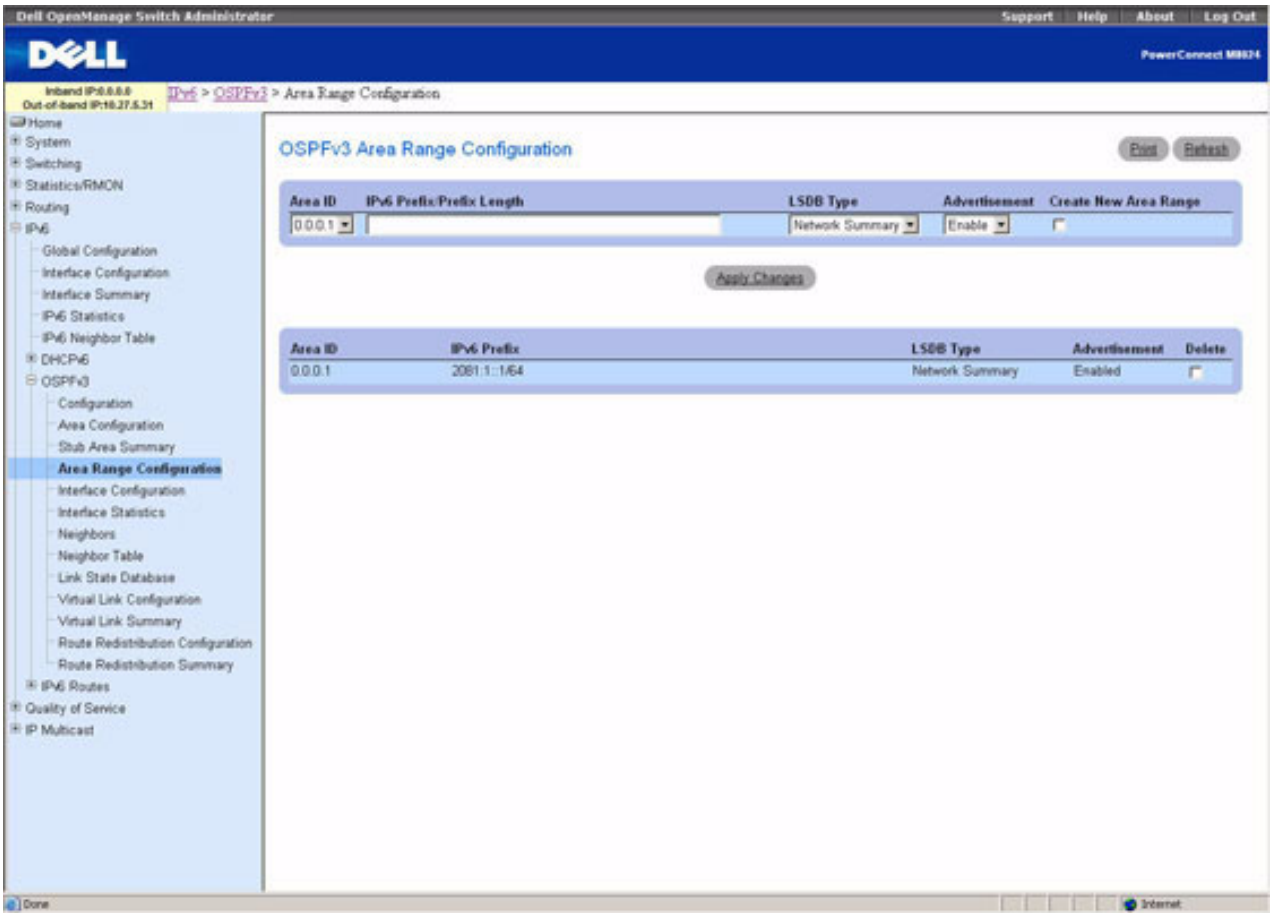
Downloaded from www.Manualslib.com manuals search engine

OSPFv3 Area Range Configuration

Use the **OSPFv3 Area Range Configuration** page to configure OSPFv3 area ranges.

To display the page, click **IPv6 > OSPFv3 > Area Range Configuration** in the tree view.

Figure 10-22. OSPFv3 Area Range Configuration



The **OSPFv3 Area Range Configuration** page contains the following fields:

- **Area ID** — Selects the area for which data is to be configured.
- **IPv6 Prefix/Prefix Length** — Enter the IPv6 Prefix/Prefix Length for the address range for the selected area.
- **LSDB Type** — Select the type of Link Advertisement associated with the specified area and address range. The default type is Network Summary.
- **Advertisement** — Select Enable or Disable from the drop-down menu. If you selected Enable, the address range is advertised outside the area through a Network Summary LSA. The default is Enable.

Downloaded from www.Manualslib.com manuals search engine

- **Create New Area Range** — Click this check box to create a new OSPFv3 area range using the values you specified.
- **Area ID** — The OSPFv3 area.
- **IPv6 Prefix** — The IPv6 Prefix of an address range for the area.
- **LSDB Type** — The Link Advertisement type for the address range and area.
- **Advertisement** — The Advertisement mode for the address range and area.
- **Delete** — Click this check box to delete the specified OSPFv3 area range.

Configuring OSPFv3 Area Range

1. Open the **OSPFv3 Area Range Configuration** page.
2. Modify the fields as needed.
3. Click **Apply Changes**.

   The OSPFv3 area range is saved, and the device is updated.

Configuring OSPFv3 Area Range using the CLI Command

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- OSPFv3 Commands

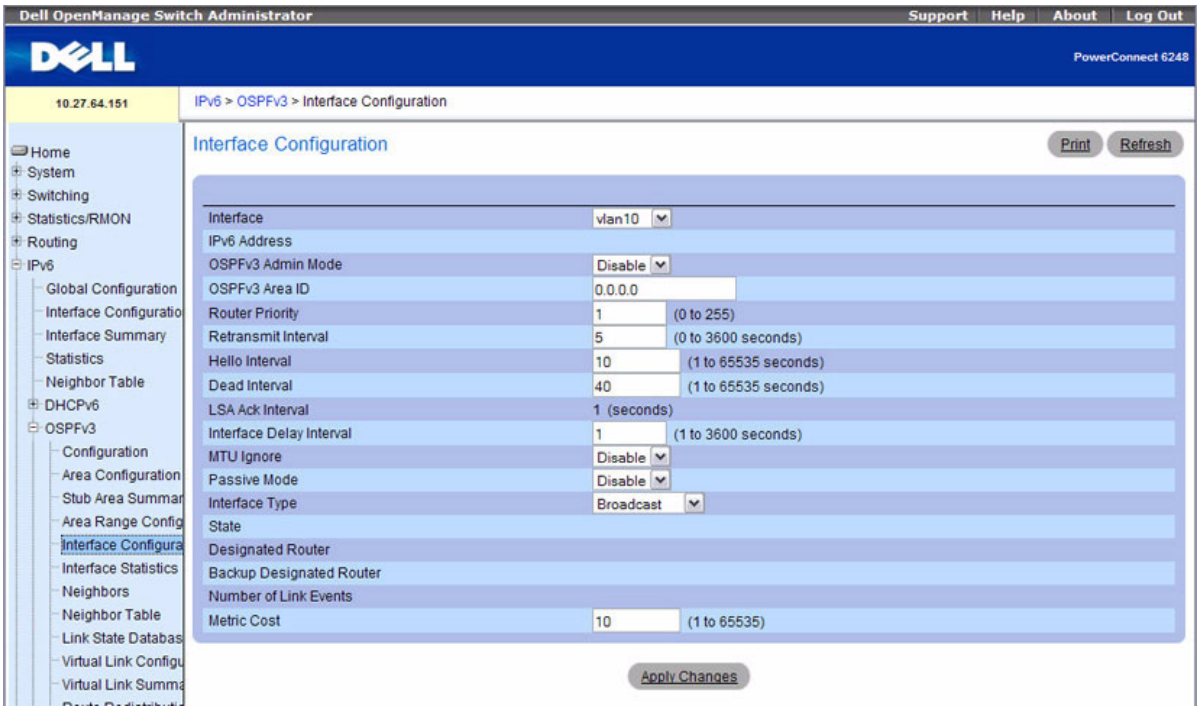
Downloaded from www.Manualslib.com manuals search engine

OSPFv3 Interface Configuration

Use the **OSPFv3 Interface Configuration** page to create and configure OSPFv3 interfaces. This page has been updated to include the Passive Mode field.

To display the page, click **IPv6 > OSPFv3 > Interface Configuration** in the tree view.

Figure 10-23. OSPFv3 Interface Configuration



The **OSPFv3 Interface Configuration** page contains the following fields:

- **Interface** — Select the interface for which data is to be displayed or configured.
- **IPv6 Address** — The IPv6 address of the interface.
- **OSPFv3 Admin Mode** — You may select Enable or Disable from the drop-down menu. The default value is Disable. You can configure OSPFv3 parameters without enabling OSPFv3 Admin Mode, but they have no effect until you enable Admin Mode. The following information is displayed only if the Admin Mode is enabled: State, Designated Router, Backup Designated Router, Number of Link Events, LSA Ack Interval, and Metric Cost. For OSPFv3 to be fully functional, the interface must have a valid IPv6 Prefix/Prefix Length. This can be done through the CLI using the `ipv6 address` command in the interface configuration mode.

NOTE: Once OSPFv3 is initialized on the router, it remains initialized until the router is reset.

- **OSPFv3 Area ID** — Enter the 32-bit integer in dotted decimal format that uniquely identifies the OSPFv3 area to which the selected router interface connects. If you assign an Area ID which does not exist, the area is created with default values.

Downloaded from www.Manualslib.com manuals search engine

- **Router Priority** — Enter the OSPFv3 priority for the selected interface. The priority of an interface is specified as an integer from 0 to 255. The default is 1, which is the highest router priority. A value of 0 indicates that the router is not eligible to become the designated router on this network.
- **Retransmit Interval** — Enter the OSPFv3 retransmit interval for the specified interface. This is the number of seconds between link-state advertisements for adjacencies belonging to this router interface. This value is also used when retransmitting database descriptions and link-state request packets. Valid values range from 0 to 3600 seconds (1 hour). The default is 5 seconds.
- **Hello Interval** — Enter the OSPFv3 hello interval for the specified interface in seconds. This parameter must be the same for all routers attached to a network. Valid values range from 1 to 65,535. The default is 10 seconds.
- **Dead Interval** — Enter the OSPFv3 dead interval for the specified interface in seconds. This specifies how long a router waits to see a neighbor router's Hello packets before declaring that the router is down. This parameter must be the same for all routers attached to a network. This value should be a multiple of the Hello Interval (for example 4). Valid values range from 1 to 165535. The default is 40.
- **LSA Ack Interval** — Displays the number of seconds between LSA Acknowledgment packet transmissions, which must be less than the Retransmit Interval.
- **Interface Delay Interval** — Enter the OSPFv3 Transit Delay for the specified interface. This specifies the estimated number of seconds it takes to transmit a link state update packet over the selected interface. Valid values range from 1 to 3600 seconds (1 hour). The default value is 1 second.
- **MTU Ignore** — Disables OSPFv3 MTU mismatch detection on receiving packets. The default value is Disable.
- Passive Mode — When you enable passive mode on an OSPFv3 interface, you disable sending OSPFv3 routing updates on the interface. An OSPFv3 adjacency will not be formed on a passive interface. Interfaces are not passive by default.
- **Interface Type** — Enter the interface type, which can either be set to broadcast mode or point to point mode. The default interface type is broadcast.
- **State** — The current state of the selected router interface. One of:
  - **Down** — This is the initial interface state. In this state, the lower-level protocols have indicated that the interface is unusable. In this state, interface parameters are set to their initial values. All interface timers are disabled, and there are no adjacencies associated with the interface.
  - **Loopback** — In this state, the router's interface to the network is looped back either in hardware or software. The interface is unavailable for regular data traffic. However, it may still be desirable to gain information on the quality of this interface, either through sending ICMP pings to the interface or through something like a bit error test. For this reason, IP packets may still be addressed to an interface in Loopback state. To facilitate this, such interfaces are advertised in router- LSAs as single host routes, whose destination is the IP interface address.

Downloaded from www.Manualslib.com manuals search engine

– **Waiting** — The router is trying to determine the identity of the (Backup) Designated Router for the network by monitoring received Hello Packets. The router is not allowed to elect a Backup Designated Router or a Designated Router until it transitions out of Waiting state. This prevents unnecessary changes of (Backup) Designated Router.

- **Designated Router** — This router is itself the Designated Router on the attached network. Adjacencies are established to all other routers attached to the network. The router must also originate a network-LSA for the network node. The network- LSA contains links to all routers (including the Designated Router itself) attached to the network.
- **Backup Designated Router** — This router is itself the Backup Designated Router on the attached network. It is promoted to Designated Router if the present Designated Router fails. The router establishes adjacencies to all other routers attached to the network. The Backup Designated Router performs slightly different functions during the Flooding Procedure, as compared to the Designated Router.
- **Other Designated Router** — The interface is connected to a broadcast or NBMA network on which other routers have been selected to be the Designated Router and Backup Designated Router either. The router attempts to form adjacencies to both the Designated Router and the Backup Designated Router.

NOTE: The State is displayed only if the OSPFv3 admin mode is enabled.

Metric Cost — Enter the value on this interface for the cost TOS (type of service). The range for the metric cost is between 1 and 65,535. Metric Cost is only configurable if OSPFv3 is initialized on the interface.

Configuring an OSPFv3 Interface

1. Open the **OSPFv3 Interface Configuration** page.
2. Select the Interface on which you want OSPFv3 configured.
3. Modify the remaining fields as needed.
4. Click **Apply Changes**.

   The interface is configured for OSPFv3, and the device is updated.

Configuring an OSPFv3 Interface using the CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- OSPFv3 Commands

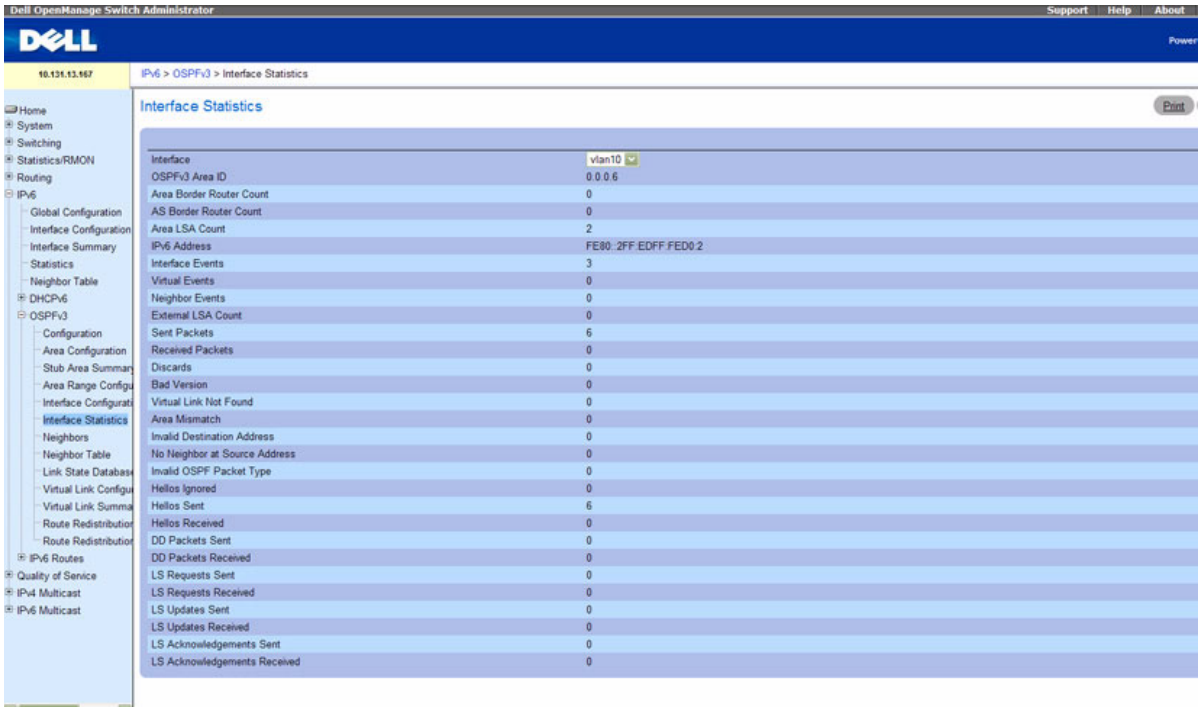
Downloaded from www.Manualslib.com manuals search engine

OSPFv3 Interface Statistics

Use the **OSPFv3 Interface Statistics** page to display OSPFv3 interface statistics. Information is only displayed if OSPF is enabled. Several fields have been added to this page.

To display the page, click **IPv6 > OSPFv3 > Interface Statistics** in the tree view.

Figure 10-24. OSPFv3 Interface Statistics



The **OSPFv3 Interface Statistics** page displays the following fields:

- **Interface** — Select the interface for which data is to be displayed.
- **OSPFv3 Area ID** — The OSPF area to which the selected router interface belongs. An OSPF Area ID is a 32-bit integer in dotted decimal format that uniquely identifies the area to which the interface connects.
- **Area Border Router Count** — The total number of area border routers reachable within this area. This is initially zero, and is calculated in each SPF Pass.
- **AS Border Router Count** — The total number of Autonomous System border routers reachable within this area. This is initially zero, and is calculated in each SPF Pass.
- **Area LSA Count** — The total number of link-state advertisements in this area's link-state database, excluding AS External LSAs.
- **IPv6 Address** - The IP address of the interface.
- **Interface Events** — The number of times the specified OSPF interface has changed its state, or an error has occurred.

Downloaded from www.Manualslib.com manuals search engine

- **Virtual Events** — The number of state changes or errors that have occurred on this virtual link.
- **Neighbor Events** — The number of times this neighbor relationship has changed state, or an error has occurred.
- **External LSA Count** — The number of external (LS type 5) link-state advertisements in the link-state database.
- **Sent packets** — The number of OSPFv3 packets transmitted on the interface.
- **Received packets** — The number of valid OSPFv3 packets received on the interface.
- **Discards** — The number of received OSPFv3 packets discarded because of an error in the packet or an error in processing the packet.
- **Bad Version** — The number of received OSPFv3 packets whose version field in the OSPFv3 header does not match the version of the OSPFv3 process handling the packet.
- **Virtual Link Not Found** — The number of received OSPFv3 packets discarded where the ingress interface is in a non-backbone area and the OSPFv3 header identifies the packet as belonging to the backbone, but OSPFv3 does not have a virtual link to the packet's sender.
- **Area Mismatch** — The number of OSPFv3 packets discarded because the area ID in the OSPFv3 header is not the area ID configured on the ingress interface.
- **Invalid Destination Address** — The number of OSPFv3 packets discarded because the packet's destination IP address is not the address of the ingress interface and is not the AllDrRouters or AllSpfRouters multicast addresses.
- **No Neighbor at Source Address** — The number of OSPFv3 packets dropped because the sender is not an existing neighbor or the sender's IP address does not match the previously recorded IP address for that neighbor.
- **Invalid OSPF Packet Type** — The number of OSPFv3 packets discarded because the packet type field in the OSPFv3 header is not a known type.
- **Hellos Ignored** — The number of received Hello packets that were ignored by this router from the new neighbors after the limit has been reached for the number of neighbors on an interface or on the system as a whole.
- **Hellos Sent** — The number of Hello packets sent on this interface by this router.
- **Hellos Received** — The number of Hello packets received on this interface by this router.
- **DD Packets Sent** — The number of Database Description packets sent on this interface by this router.
- **DD Packets Received** — The number of Database Description packets received on this interface by this router.
- **LS Requests Sent** — The number of LS Requests sent on this interface by this router.
- **LS Requests Received** — The number of LS Requests received on this interface by this router.
- **LS Updates Sent** — The number of LS updates sent on this interface by this router.
- **LS Updates Received** — The number of LS updates received on this interface by this router.

Downloaded from www.Manualslib.com manuals search engine

- **LS Acknowledgements Sent** — The number of LS acknowledgements sent on this interface by this router.
- **LS Acknowledgements Received** — The number of LS acknowledgements received on this interface by this router.

Displaying OSPFv3 Interface Statistics

1. Open the **OSPFv3 Interface Statistics** page.
2. Select the interface to display from the **Interface** drop-down menu.

   Statistics for the interface display.

Displaying OSPFv3 Interface Statistics using the CLI Command

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- OSPFv3 Commands

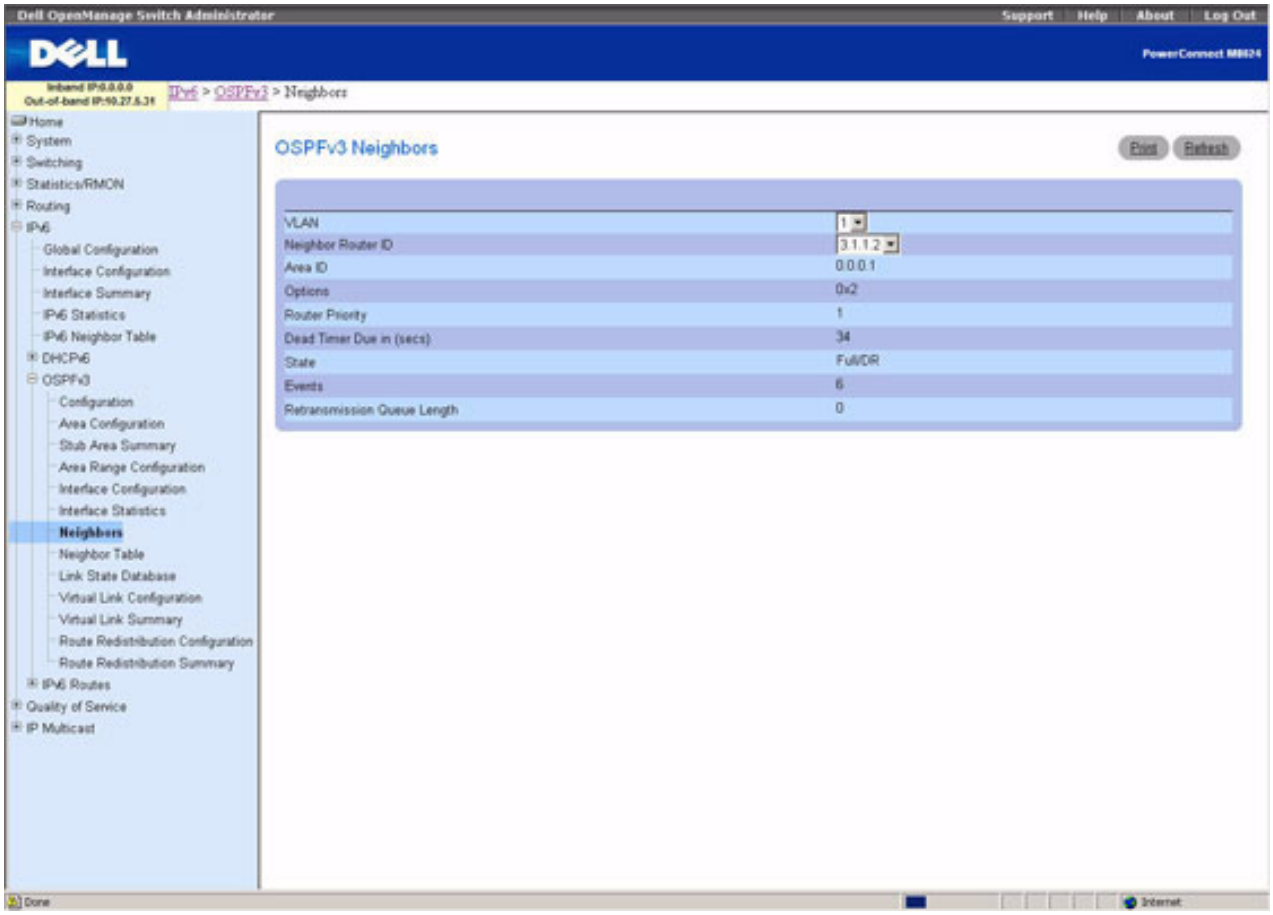
OSPFv3 Neighbors

Use the **OSPFv3 Neighbors** page to display the OSPF neighbor configuration for a selected neighbor ID. When a particular neighbor ID is specified, detailed information about that neighbor is given. Neighbor information only displays if OSPF is enabled and the interface has a neighbor. The IP address is the IP address of the neighbor.

To display the page, click **IPv6 > OSPFv3 > Neighbors** in the tree view.

Downloaded from www.Manualslib.com manuals search engine

Figure 10-25. OSPFv3 Neighbors



The **OSPFv3 Neighbors** page contains the following fields:

- **Interface** — Selects the interface for which data is to be displayed or configured.
- **Neighbor Router ID** — Selects the IP Address of the neighbor for which data is to be displayed.
- **Area ID** — A 32-bit integer in dotted decimal format that identifies the neighbor router.
- **Options** — The optional OSPF capabilities supported by the neighbor. The neighbor's optional OSPF capabilities are also listed in its Hello packets. This enables received Hello Packets to be rejected (i.e., neighbor relationships do not even start to form) if there is a mismatch in certain crucial OSPF capabilities.
- **Router Priority** — Displays the OSPF priority for the specified neighbor. The priority of a neighbor is a priority integer from 0 to 255. A value of 0 indicates that the router is not eligible to become the designated router on this network.
- **Dead Timer Due in (secs)** — If Hello packets do not arrive, specifies amount of time elapsed before neighbor is declared dead.

Downloaded from www.Manualslib.com manuals search engine

- **State** — The state of a neighbor can be the following:
  - **Down** — This is the initial state of a neighbor conversation. It indicates that there is no recent information received from the neighbor. On NBMA networks, Hello packets may still be sent to Down neighbors, although at a reduced frequency.
  - **Attempt** — This state is only valid for neighbors attached to NBMA networks. It indicates that no recent information has been received from the neighbor, but that a more concerted effort should be made to contact the neighbor. This is done by sending the neighbor Hello packets at intervals of Hello Interval.
  - **Init** — In this state, a Hello packet has recently been seen from the neighbor. However, bidirectional communication has not yet been established with the neighbor (i.e., the router itself did not appear in the neighbor's Hello packet). All neighbors in this state (or greater) are listed in the Hello packets sent from the associated interface.
  - **2-Way** — In this state, communication between the two routers is bidirectional. This has been assured by the operation of the Hello Protocol. This is the most advanced state short of beginning adjacency establishment. The (Backup) Designated Router is selected from the set of neighbors in state 2-Way or greater.
  - **Exchange Start** — This is the first step in creating an adjacency between the two neighboring routers. The goal of this step is to decide which router is the master, and to decide upon the initial DD sequence number. Neighbor conversations in this state or greater are called adjacencies.
  - **Exchange** — In this state the router is describing its entire link state database by sending Database Description packets to the neighbor. In this state, Link State Request Packets may also be sent asking for the neighbor's more recent LSAs. All adjacencies in Exchange state or greater are used by the flooding procedure. These adjacencies are fully capable of transmitting and receiving all types of OSPF routing protocol packets.
  - **Loading** — In this state, Link State Request packets are sent to the neighbor asking for the more recent LSAs that have been discovered (but not yet received) in the Exchange state.
  - **Full** — In this state, the neighboring routers are fully adjacent. These adjacencies now appears in router-LSAs and network-LSAs.
- **Events** — The number of times this neighbor relationship has changed state, or an error has occurred.
- **Retransmission Queue Length** — The current length of the retransmission queue.

Displaying OSPFv3 Neighbors

1. Open the **OSPFv3 Neighbors** page.
2. Select the interface to display from the **Interface** drop-down menu.
3. Select the **Neighbor Router ID** to display.

   Statistics for the selected interface **Neighbor ID** display.

Downloaded from www.Manualslib.com manuals search engine

Displaying OSPFv3 Neighbors using the CLI Command

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

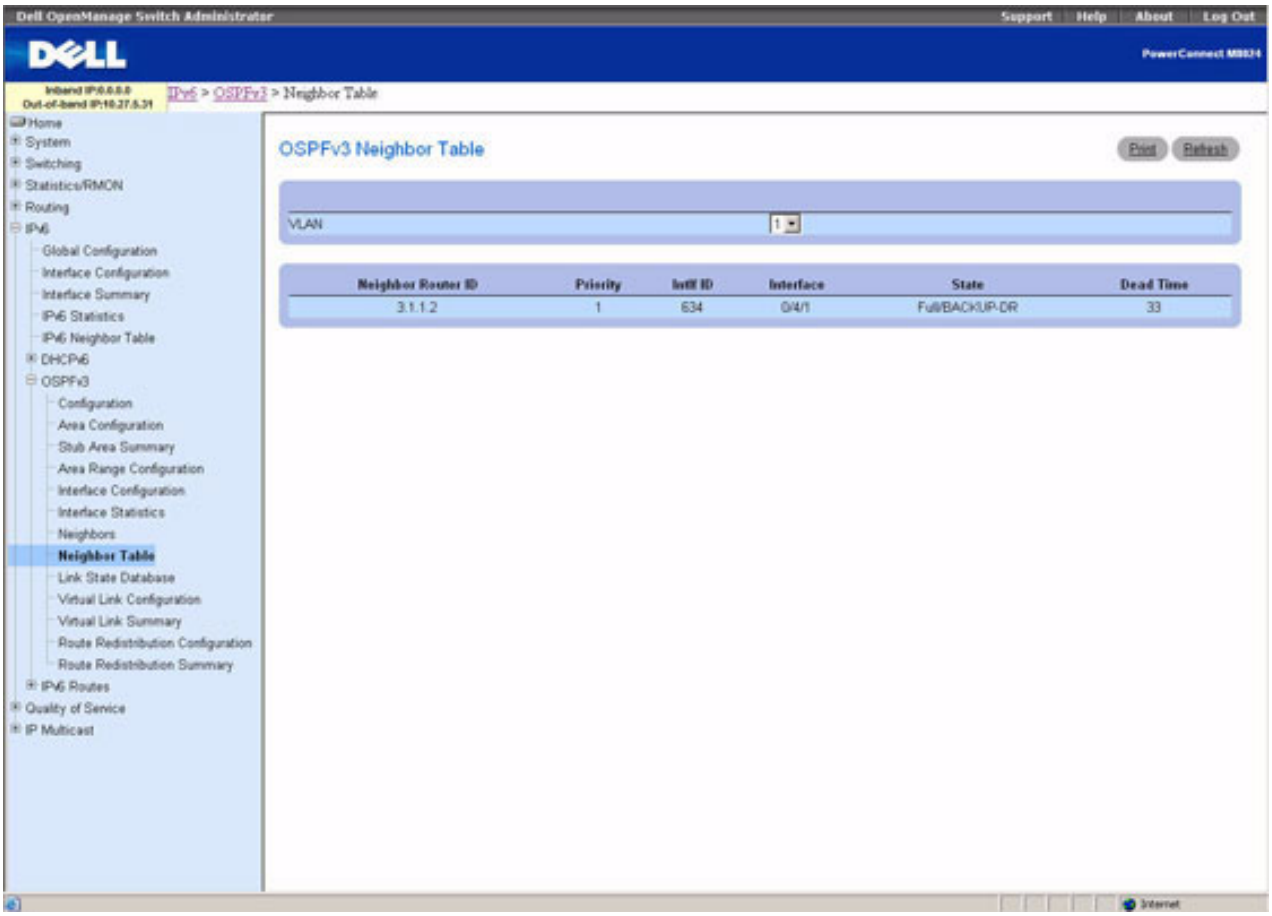
- OSPFv3 Commands

OSPFv3 Neighbor Table

Use the **OSPFv3 Neighbor Table** page to display the OSPF neighbor table list. When a particular neighbor ID is specified, detailed information about a neighbor is given. The neighbor table is only displayed if OSPF is enabled.

To display the page, click **IPv6 > OSPFv3 > Neighbor Table** in the tree view.

Figure 10-26. OSPFv3 Neighbor Table



Downloaded from www.Manualslib.com manuals search engine

The **OSPFv3 Neighbor Table** page displays the following fields:

- **Interface** — Selects the interface for which data is to be displayed or configured.
- **Neighbor Router ID** — A 32-bit integer in dotted decimal format representing the neighbor interface.
- **Priority** — The priority of this neighbor in the designated router election algorithm. A value of 0 indicates that the neighbor is not eligible to become the designated router on this network.
- **IntlfID** — The Interface ID that the neighbor advertises in its Hello packets on this link.
- **Interface** — The slot/port that identifies the neighbor interface index.
- **State** — State of the relationship with this neighbor.
- **Dead Time** — Number of seconds since last Hello was received from adjacent neighbors. Set this value to 0 for neighbors in a state less than or equal to Init.

Displaying the OSPFv3 Neighbor Table

1. Open the **OSPFv3 Neighbor Table** page.
2. Select the interface to display from the **Interface** drop-down menu.

   The OSPF neighbor table for the selected interface displays.

Displaying the OSPFv3 Neighbor Table using the CLI Command

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- OSPFv3 Commands

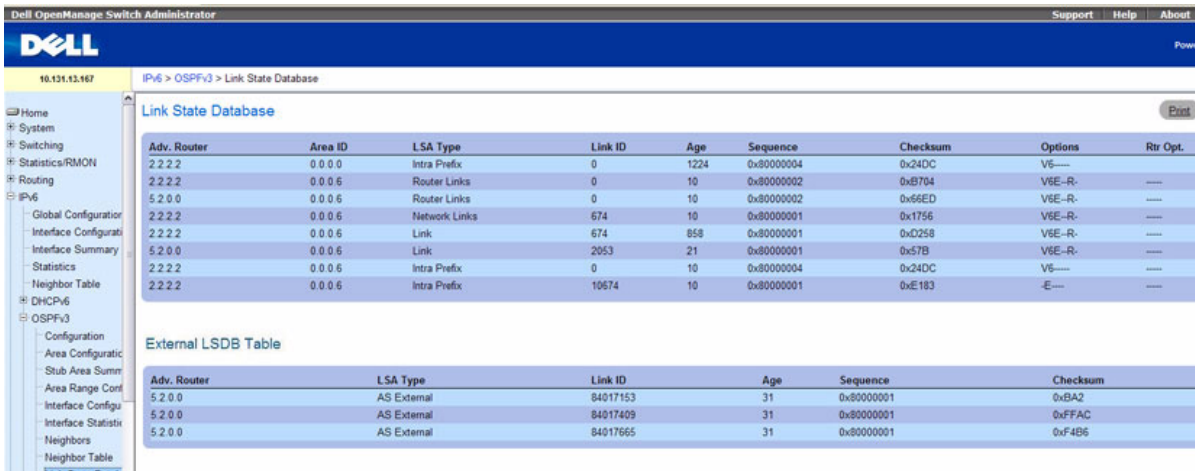
Downloaded from www.Manualslib.com manuals search engine

OSPFv3 Link State Database

Use the **OSPFv3 Link State Database** page to display the link state and external LSA databases. The OSPFv3 **Link State Database** page has been updated to display external LSDB table information in addition to OSPFv3 link state information.

To display the page, click **IPv6 > OSPFv3 > Link State Database** in the tree view.

Figure 10-27. OSPFv3 Link State Database



The **OSPFv3 Link State Database** page displays the following fields:

- **Adv. Router** — The 32-bit integer in dotted decimal format that uniquely identifies the router within the autonomous system (AS). The Router ID is set on the OSPFv3 Configuration page.
- **Area ID** — The ID of an OSPF area to which one of the router interfaces is connected. An Area ID is a 32-bit integer in dotted decimal format that uniquely identifies the area to which an interface is connected.
- **LSA Type** — The format and function of the link state advertisement. The types, which are defined in RFC 2740 section A.4, can be any of the following:
  - Router-LSA
  - Network-LSA
  - Inter-Area-Prefix-LSA
  - Inter-Area-Router-LSA
  - AS-External-LSA
  - Type-7-LSA
  - Link-LSA
  - Intra-Area-Prefix-LSA
- **Link ID** — The Link State ID identifies the piece of the routing domain that is being described by the advertisement. The value of the LS ID depends on the advertisement's LS type.

Downloaded from www.Manualslib.com manuals search engine

- **Age** — The time since the link state advertisement was first originated, in seconds.
- **Sequence** — The sequence number field is a signed 32-bit integer. It is used to detect old and duplicate link state advertisements. The larger the sequence number, the more recent the advertisement.
- **Checksum** — The checksum is used to detect data corruption of an advertisement. This corruption can occur while an advertisement is being flooded, or while it is being held in a router's memory. This field is the checksum of the complete contents of the advertisement, except the LS age field.
- **Options** — The Options field in the link state advertisement header indicates which optional capabilities are associated with the advertisement. The options are:
  - V6 — When clear, the link is excluded from IPv6 routing calculations.
  - E — Describes how AS-external-LSAs are flooded
  - MC — Describes whether IP multicast datagrams are forwarded according to the specifications in
  - N — Describes how Type-7 LSAs are handled
  - R — Shows whether the originator is an active router. The R option is the router bit, and when it is clear, routes that pass through the advertising node cannot be computed.
  - DC — Describes how the system handles demand circuits.

Rtr Opt. — Shows router-specific options.

Displaying OSPFv3 Link State Database using the CLI Command

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- OSPFv3 Commands

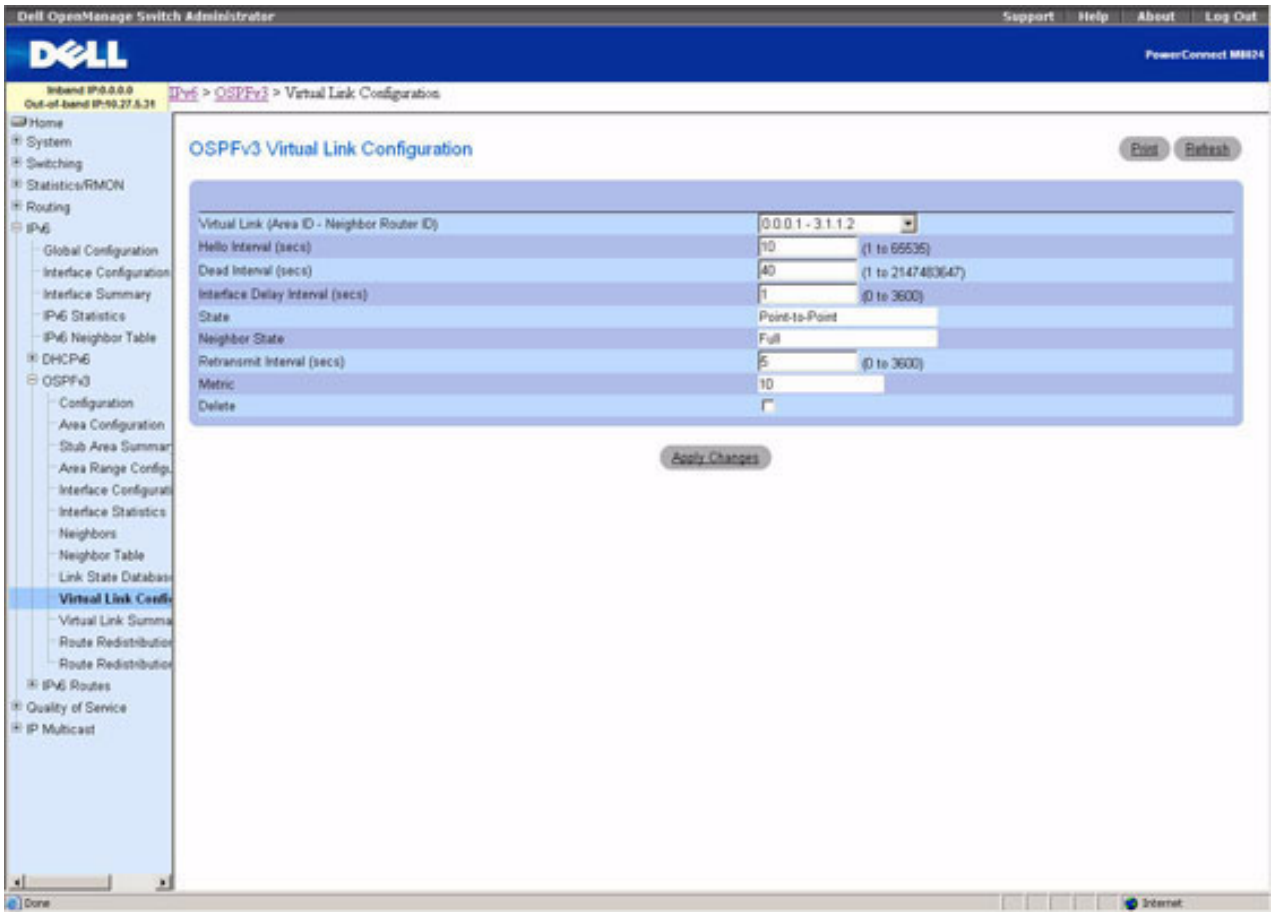
Downloaded from www.Manualslib.com manuals search engine

OSPFv3 Virtual Link Configuration

Use the **OSPFv3 Virtual Link Configuration** page to define a new or configure an existing virtual link. To display this page, a valid OSPFv3 area must be defined through the OSPFv3 Area Configuration page.

To display the page, click **IPv6 > OSPFv3 > Virtual Link Configuration** in the tree view.

Figure 10-28. OSPFv3 Virtual Link Configuration



The **OSPFv3 Virtual Link Configuration** page contains the following fields:

- **Create New Virtual Link** — Select this option from the drop-down menu to define a new virtual link. The area portion of the virtual link identification is fixed: you are prompted to enter the Neighbor Router ID on a new screen.
- **Virtual Link (Area ID - Neighbor Router ID)** — Select the virtual link for which you want to display or configure data. It consists of the Area ID and Neighbor Router ID.
- **Hello Interval (secs)** — Enter the OSPF hello interval for the specified interface in seconds. This parameter must be the same for all routers attached to a network. Valid values range from 1 to 65,535. The default is 10 seconds.

Downloaded from www.Manualslib.com manuals search engine

- **Dead Interval (secs)** — Enter the OSPF dead interval for the specified interface in seconds. This specifies how long a router waits to see a neighbor router's Hello packets before declaring that the router is down. This parameter must be the same for all routers attached to a network. This value should be a multiple of the Hello Interval (for example 4). Valid values range from 1 to 2147483647. The default is 40.
- **Interface Delay Interval (secs)** — Enter the OSPF Transit Delay for the specified interface. This specifies the estimated number of seconds it takes to transmit a link state update packet over the selected interface. Valid values range from 1 to 3600 seconds (1 hour). The default value is 1 second.
- **State** — The current state of the selected Virtual Link. One of:
  - **Down** — This is the initial interface state. In this state, the lower-level protocols have indicated that the interface is unusable. In this state, interface parameters are set to their initial values. All interface timers are disabled, and there are no adjacencies associated with the interface.
  - **Waiting** — The router is trying to determine the identity of the (Backup) Designated Router by monitoring received Hello Packets. The router is not allowed to elect a Backup Designated Router or a Designated Router until it transitions out of Waiting state. This prevents unnecessary changes of (Backup) Designated Router.
  - **Point-to-Point** — The interface is operational, and is connected either to the virtual link. On entering this state the router attempts to form an adjacency with the neighboring router. Hello Packets are sent to the neighbor every HelloInterval seconds.
  - **Designated Router** — This router is itself the Designated Router on the attached network. Adjacencies are established to all other routers attached to the network. The router must also originate a network-LSA for the network node. The network- LSA contains links to all routers (including the Designated Router itself) attached to the network.
  - **Backup Designated Router** — This router is itself the Backup Designated Router on the attached network. It is promoted to Designated Router if the present Designated Router fails. The router establishes adjacencies to all other routers attached to the network. The Backup Designated Router performs slightly different functions during the Flooding Procedure, as compared to the Designated Router.
  - **Other Designated Router** — The interface is connected to a broadcast or NBMA network on which other routers have been selected to be the Designated Router and Backup Designated Router either. The router attempts to form adjacencies to both the Designated Router and the Backup Designated Router.
- **Neighbor State** — The state of the Virtual Neighbor Relationship.
- **Retransmit Interval** — Enter the OSPF retransmit interval for the specified interface. This is the number of seconds between link-state advertisements for adjacencies belonging to this router interface. This value is also used when retransmitting database descriptions and link-state request packets. Valid values range from 1 to 3600 seconds (1 hour). The default is 5 seconds.
- **Metric** — The metric value used by the virtual link.
- **Delete** — Removes the specified virtual link from the router configuration.

Downloaded from www.Manualslib.com manuals search engine

Creating a New Virtual Link

1. Open the **OSPFv3 Virtual Link Configuration** page.
2. Select **Create New Virtual Link** from the drop-down menu to define a new virtual link.
3. Enter the **Neighbor Router ID**.
4. Click **Create**.

   The new link is created, and you are returned to the Virtual Link Configuration page.

Configuring a Virtual Link

1. Open the **OSPFv3 Virtual Link Configuration** page.
2. Select the virtual link to configure.
3. Modify the remaining fields as needed.
4. Click **Apply Changes**.
5. The virtual link is configured for OSPFv3, and the device is updated.

Configuring an OSPFv3 Virtual Link using CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- OSPFv3 Commands

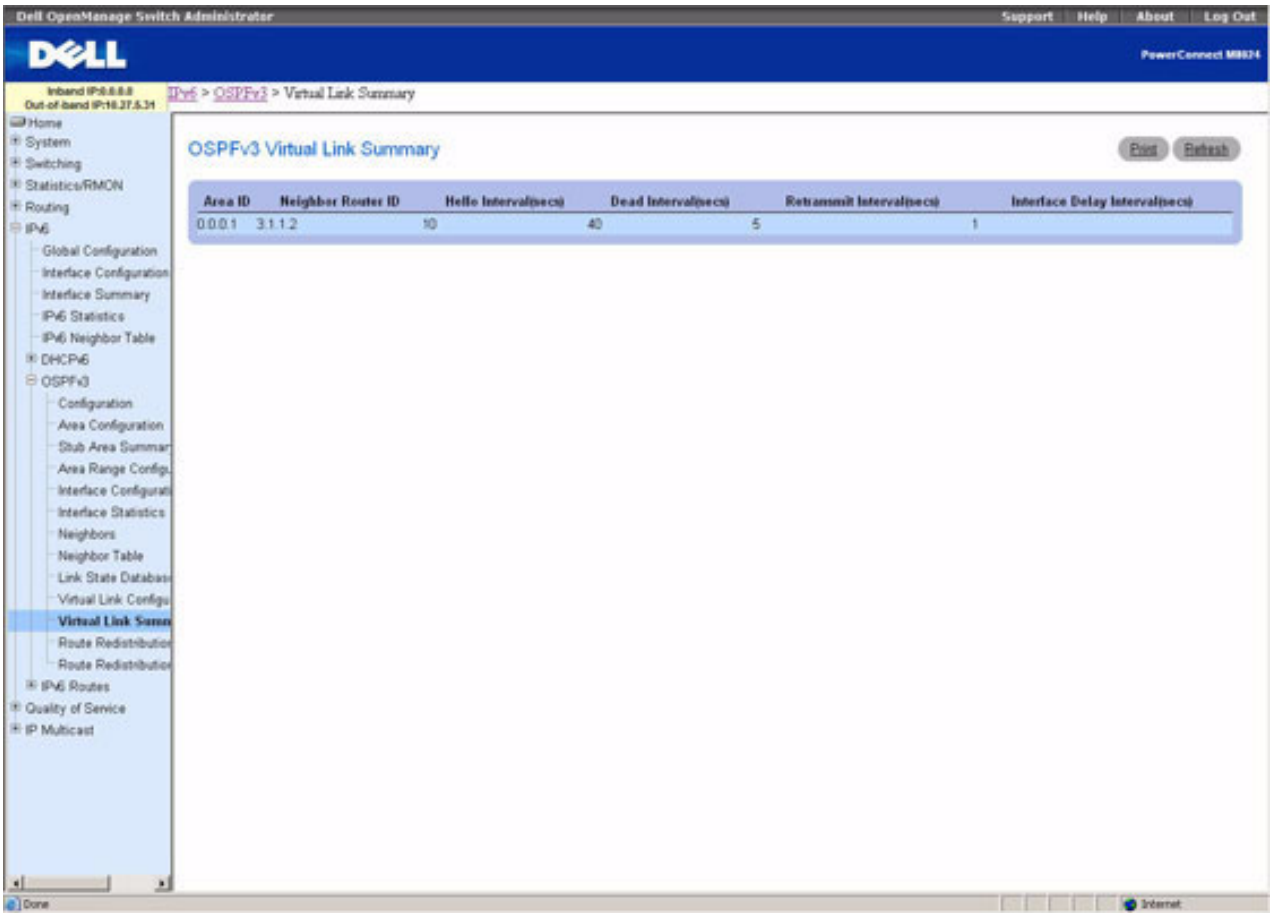
Downloaded from www.Manualslib.com manuals search engine

OSPFv3 Virtual Link Summary

Use the **OSPFv3 Virtual Link Summary** page to display virtual link data by Area ID and Neighbor Router ID.

To display the page, click **IPv6 > OSPFv3 > Virtual Link Summary** in the tree view.

Figure 10-29. OSPFv3 Virtual Link Summary



The **OSPFv3 Virtual Link Summary** page displays the following fields:

- **Area ID** — The Area ID portion of the virtual link identification for which data is to be displayed. The Area ID and Neighbor Router ID together define a virtual link.
- **Neighbor Router ID** — The neighbor portion of the virtual link identification. Virtual links may be configured between any pair of area border routers having interfaces to a common (non-backbone) area.
- **Hello Interval (secs)** — The OSPF hello interval for the virtual link in units of seconds. The value for hello interval must be the same for all routers attached to a network.

Downloaded from www.Manualslib.com manuals search engine

- **Dead Interval (secs)** — The OSPF dead interval for the virtual link in units of seconds. This specifies how long a router waits to see a neighbor router's Hello packets before declaring that the router is down. This parameter must be the same for all routers attached to a common network, and should be a multiple of the Hello Interval (i.e. 4).
- **Retransmit Interval (secs)** — The OSPF retransmit interval for the virtual link in units of seconds. This specifies the time between link-state advertisements for adjacencies belonging to this router interface. This value is also used when retransmitting database descriptions and link-state request packets.
- **Interface Delay Interval (secs)** — The OSPF Transit Delay for the virtual link in units of seconds. It specifies the estimated number of seconds it takes to transmit a link state update packet over this interface.

Displaying OSPFv3 Virtual Link Summary using the CLI Command

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

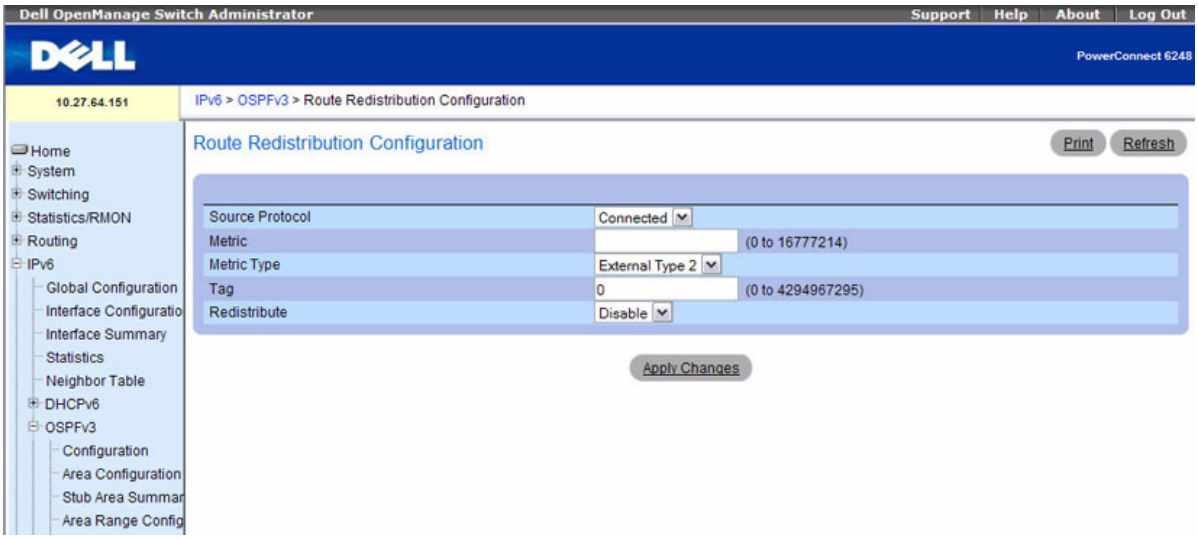
- OSPFv3 Commands

OSPFv3 Route Redistribution Configuration

Use the **OSPFv3 Route Redistribution Configuration** page to configure route redistribution.

To display the page, click **IPv6 > OSPFv3 > Route Redistribution Configuration** in the tree view.

Figure 10-30. OSPFv3 Route Redistribution Configuration



Downloaded from www.Manualslib.com manuals search engine

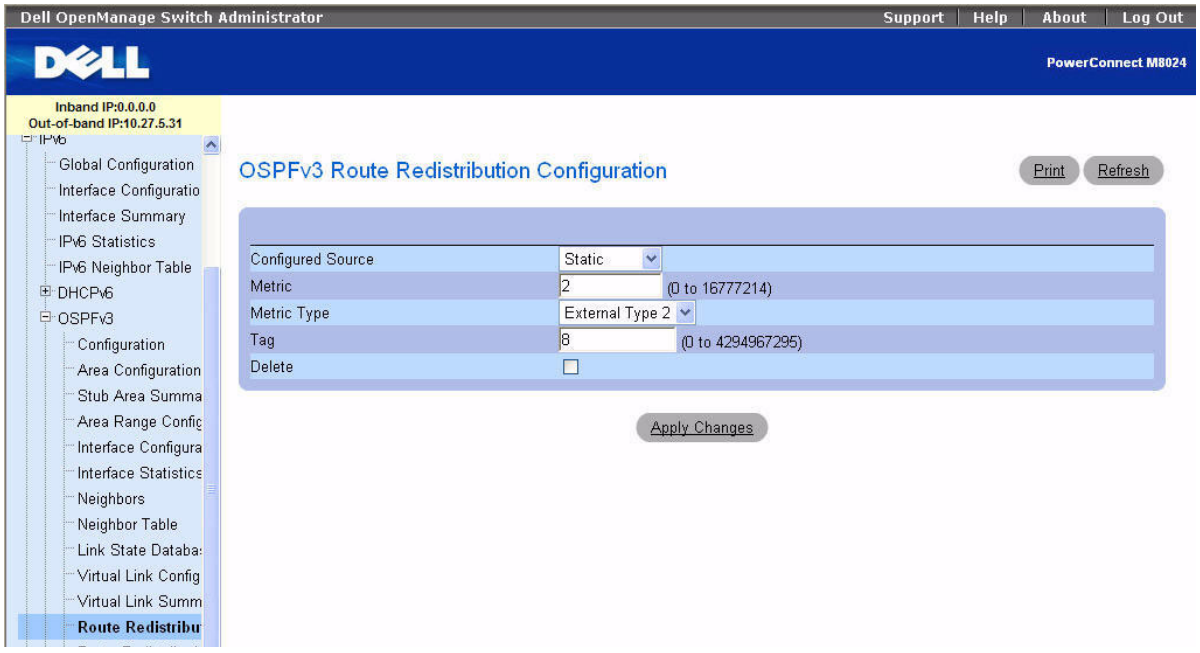
The **OSPFv3 Route Redistribution Configuration** page contains the following fields:

- **Source Protocol** — Select the type of source routes to configure for redistribution by OSPF. Valid values are Static and Connected.
- **Metric** — Sets the metric value to be used as the metric of redistributed routes. This field displays the metric if the source was pre-configured and can be modified. Valid values are 0 to 16777214.
- **Metric Type** — Sets the OSPF metric type of redistributed routes.
- **Tag** — Sets the tag field in routes redistributed. This field displays the tag if the source was pre-configured, otherwise 0 is displayed. Valid values are 0 to 4294967295.
- **Redistribute** — Enables or disables the redistribution for the selected source protocol. This field has to be enabled in order to be able to configure any of the route redistribution attributes.

Configuring OSPFv3 Route Redistribution

1. Open the **OSPFv3 Route Redistribution Configuration** page.
2. Specify **Create** to set up a new configured source. Specify **Connected** or **Static** to modify an existing configured source.

Figure 10-31. OSPFv3 Route Redistribution Configuration - Configured Source



3. Set up or modify the remaining fields as needed.
4. Click **Apply Changes**.

   The selected route redistribution is configured for OSPFv3, and the device is updated.

Downloaded from www.Manualslib.com manuals search engine

Configuring OSPFv3 Route Redistribution using the CLI Command

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

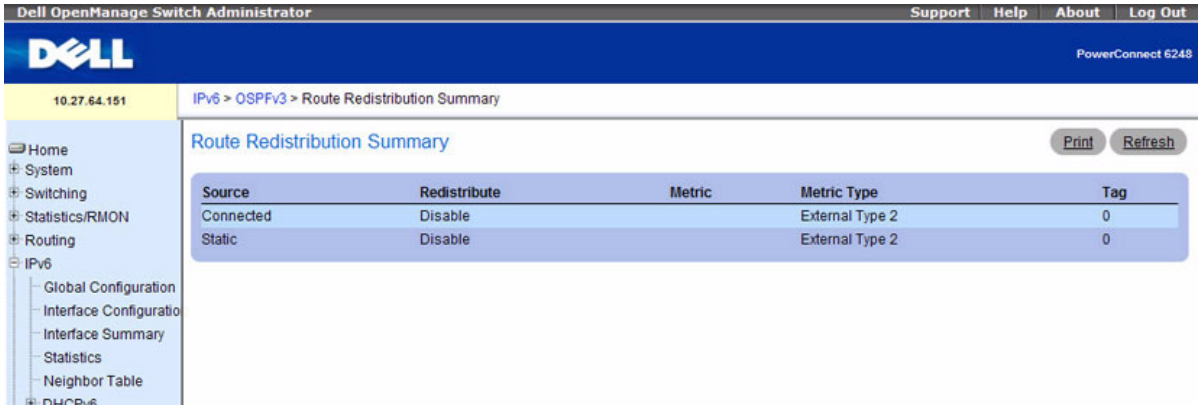
- OSPFv3 Commands

OSPFv3 Route Redistribution Summary

Use the **OSPFv3 Route Redistribution Summary** page to display route redistribution settings by source.

To display the page, click **IPv6 > OSPFv3 > Route Redistribution Summary** in the tree view.

Figure 10-32. OSPFv3 Route Redistribution Summary



The **OSPFv3 Route Redistribution Summary** page displays the following fields:

- **Source** — The Source Route to be Redistributed by OSPF.
- **Redistribute** — Specify whether to allow the routes learned through this protocol to be redistributed.
- **Metric** — The Metric of redistributed routes for the given Source Route. Displays nothing when not configured.
- **Metric Type** — The OSPF metric type of redistributed routes.
- **Tag** — The tag field in routes redistributed. This field displays the tag if the source was pre-configured, otherwise 0.

Displaying OSPFv3 Route Redistribution Summary using the CLI Command

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- OSPFv3 Commands

Downloaded from www.Manualslib.com manuals search engine

IPv6 Routes

The **IPv6 Routes** menu page contains links to web pages that define and display IPv6 Routes parameters and data. To display this page, click **IPv6 > IPv6 Routes** in the tree view. Following are the web pages accessible from this menu page:

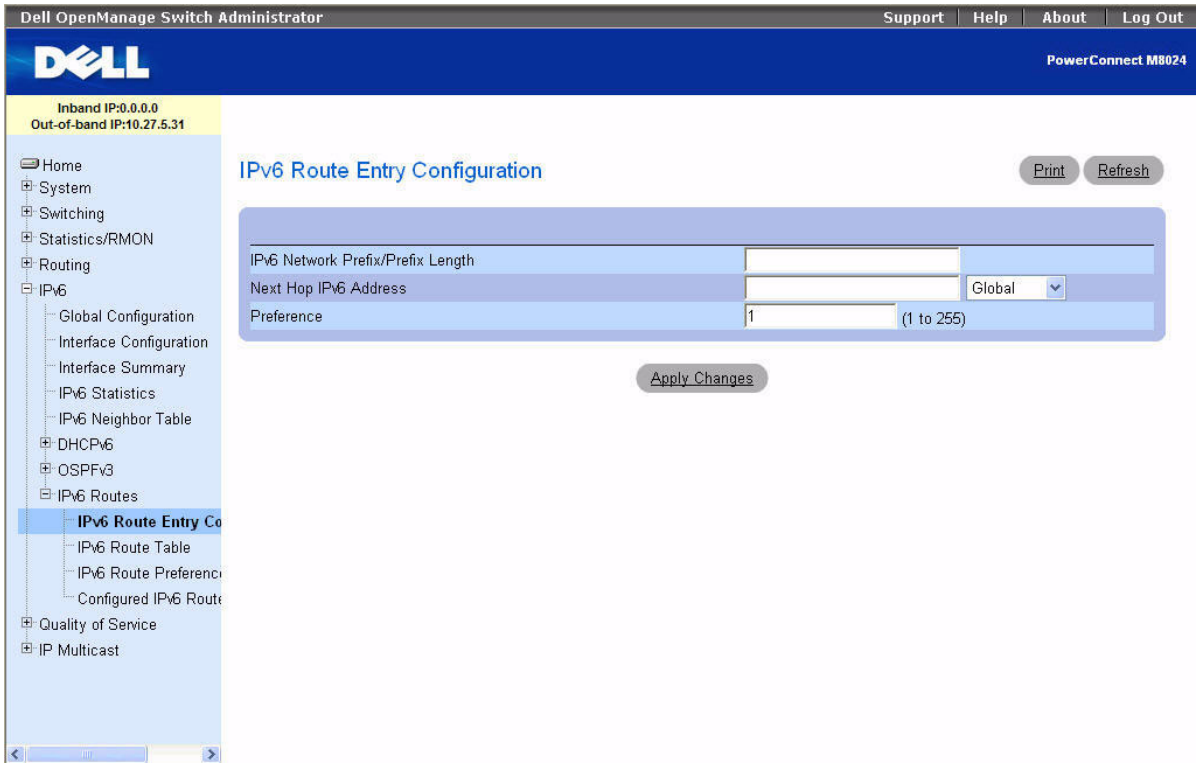
- IPv6 Route Entry Configuration
- IPv6 Route Table
- IPv6 Route Preferences
- Configured IPv6 Routes

IPv6 Route Entry Configuration

Use the **IPv6 Route Entry Configuration** page to configure information for IPv6 routes.

To display the page, click **IPv6 > IPv6 Routes > IPv6 Route Entry Configuration** in the tree view.

Figure 10-33. IPv6 Route Entry Configuration



Downloaded from www.Manualslib.com manuals search engine

The **IPv6 Route Entry Configuration** page contains the following fields:

- **IPv6 Network Prefix/PrefixLength** — Enter a valid IPv6 Network Address and Prefix.
- **Next Hop IPv6 Address** — Enter an IPv6 Next Hop Address. If the Next Hop IPv6 Address specified is a Link-local IPv6 Address, specify the Interface for the Link-local IPv6 Next Hop Address. Select Global or Link-local from the drop-down menu to apply to this address.
- **Preference** — Enter a Preference Value for the given route. Valid values are 1 to 255, with the default as 1.

Configuring IPv6 Route Entry

1. Open the **IPv6 Route Entry Configuration** page.
2. Modify the fields as needed.
3. Click **Apply Changes**.

   The route entry is configured for IPv6, and the device is updated.

Configuring Route Entry the CLI Command

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- IPv6 Routing Commands

Downloaded from www.Manualslib.com manuals search engine

IPv6 Route Table

Use the **IPv6 Route Table** page to display all active IPv6 routes and their settings.

To display the page, click **IPv6 > IPv6 Routes > IPv6 Route Table** in the tree view.

Figure 10-34. IPv6 Route Table

The **IPv6 Route Table** page displays the following fields:

- **Routes Displayed** — Select to view either the Configured Routes, Best Routes, or All Routes from the drop-down menu.
- **Number of Routes** — Displays the total number of active routes/best routes in the route table for the type of route selected.
- **IPv6 Prefix/Prefix Length** — Displays the Network Prefix and Prefix Length for the Active Route.
- **Protocol** — Displays the Type of Protocol for the Active Route.
- **Next Hop Interface** — Displays the Interface over which the Route is Active.
- **Next Hop IP Address** — Displays the Next Hop IPv6 Address for the Active Route.

Downloaded from www.Manualslib.com manuals search engine

Displaying the IPv6 Route Table

1. Open the **IPv6 Route Table** page.
2. Select the type of routes to display from the **Routes Displayed** field.

   The selected routes display.

Displaying the IPv6 Route Table using the CLI Command

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- IPv6 Routing Commands

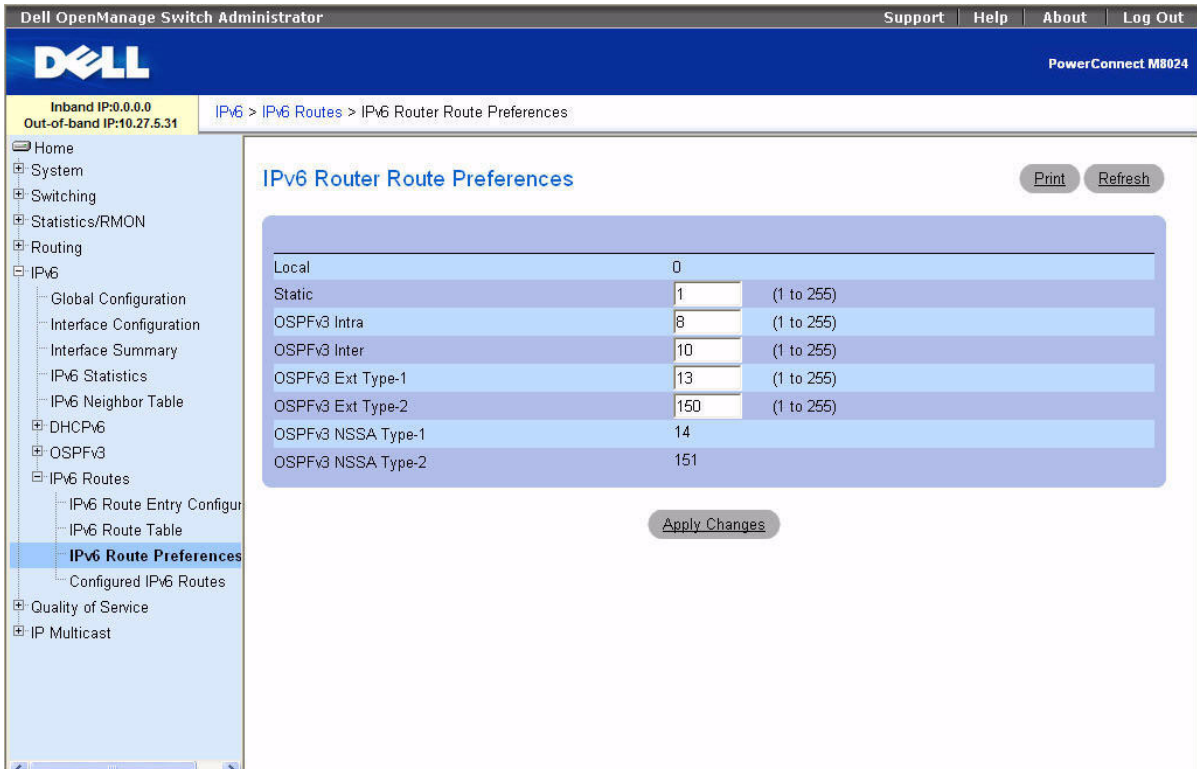
IPv6 Route Preferences

Use the **IPv6 Route Preferences** page to configure the default preference for each protocol. These values are arbitrary values in the range of 1 to 255 and are independent of route metrics. Most routing protocols use a route metric to determine the shortest path known to the protocol, independent of any other protocol. The best route to a destination is chosen by selecting the route with the lowest preference value. When there are multiple routes to a destination, the preference values are used to determine the preferred route. If there is still a tie, the route with the best route metric is chosen. To avoid problems with mismatched metrics you must configure different preference values for each of the protocols.

To display the page, click **IPv6 > IPv6 Routes > IPv6 Route Preferences** in the tree view.

Downloaded from www.Manualslib.com manuals search engine

Figure 10-35. IPv6 Route Preferences



The **IPv6 Route Preferences** page contains the fields shown below. In each case, the lowest values indicate the highest preference.

- **Local** — This field displays the local route preference value.
- **Static** — The static route preference value in the router. The default value is 1. The range is 1 to 255.
- **OSPF Intra** — The OSPF intra route preference value in the router. The default value is 110.
- **OSPF Inter** — The OSPF inter route preference value in the router. The default value is 110.
- **OSPF External** — The OSPF External route preference value in the router (OSPF Type-1 and OSPF Type-2 routes). The default value is 110.

Configuring IPv6 Route Preferences

1. Open the **IPv6 Route Preferences** page.
2. Configure the default preference for each protocol.
3. Click **Apply Changes**.

   Route preferences are configured for IPv6, and the device is updated.

Downloaded from www.Manualslib.com manuals search engine

Configuring IPv6 Route Preferences using the CLI Command

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

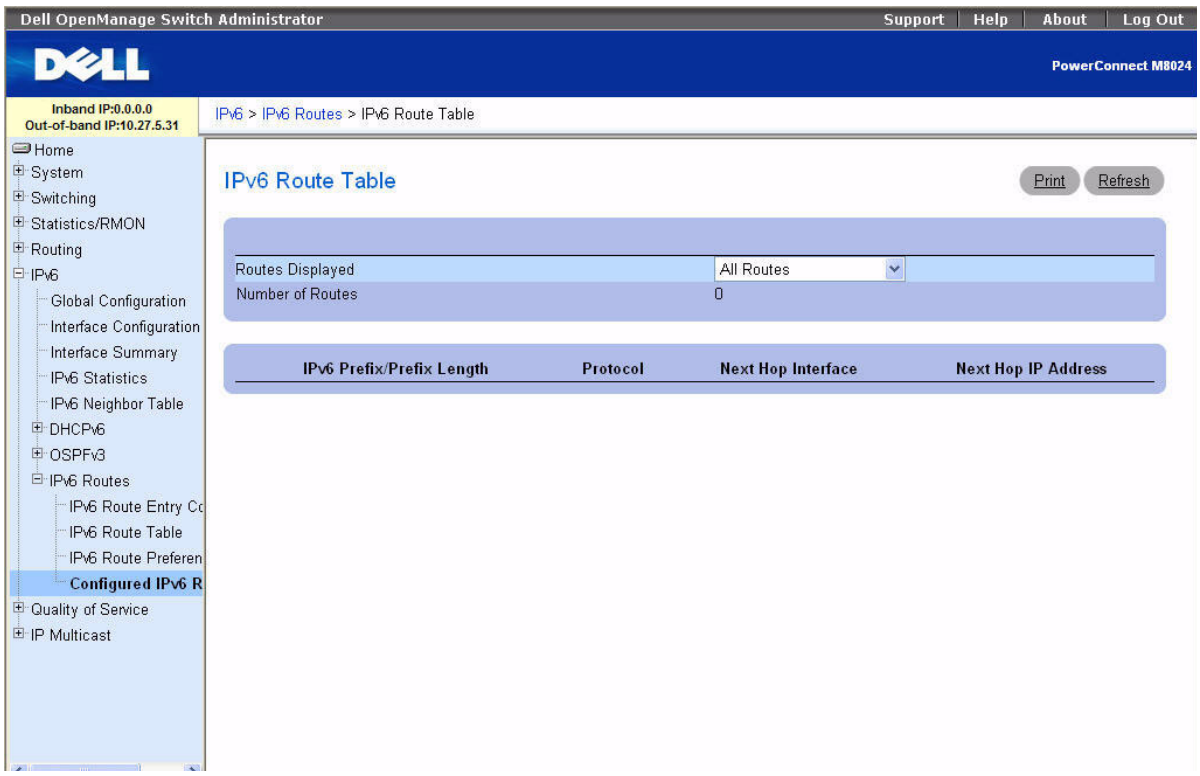
- IPv6Routing Commands

Configured IPv6 Routes

Use the **Configured IPv6 Routes** page to display selected IPv6 routes.

To display the page, click **IPv6 > IPv6 Routes > Configured IPv6 Routes** in the tree view.

Figure 10-36. Configured IPv6 Routes



The **Configured IPv6 Routes** page contains the following fields:

- **Routes Displayed** — Select to view either the Configured Routes, Best Routes or All Routes.

When the Configured Routes option is selected, the following fields appear:

- **IPv6 Prefix/Prefix Length** — Displays the Network Prefix and Prefix Length for the Configured Route.
- **Next Hop IP** — Displays the Next Hop IPv6 Address for the Configured Route.
- **Next Hop Interface** — Displays the Next Hop Interface for the Configured Route.
- **Preference** — Displays the Route Preference of the Configured Route.

Downloaded from www.Manualslib.com manuals search engine

- **Delete** — Click this box and the Refresh button to delete the displayed route.

When the Best Routes or All Routes options are select, the following fields appear:

- **Number of Routes** — Displays the number of Best Routes or All Routes.
- **IPv6 Prefix/Prefix Length** — Displays the Network Prefix and Prefix Length for the Configured Route.
- **Protocol** — Displays the protocol in use for the Configured routes.
- **Next Hop Interface** — Displays the Next Hop Interface for the Configured Route.
- **Next Hop IP** Address — Displays the Next Hop IPv6 Address for the Configured Route.

Displaying IPv6 Routes

1. Open the **Configured IPv6 Routes** page.
2. Select the routes to view from the **Routes Displayed** drop-down menu.

   The selected routes and their configurations display.

Displaying IPv6 Routes using the CLI Command

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide*:

- IPv6 Routing Commands

Downloaded from www.Manualslib.com manuals search engine

11

Configuring Quality of Service

Quality of Service Overview

This section gives an overview of Quality of Service (QoS) and explains the QoS features available from the Quality of Service menu page—Differentiated Services and Class of Service.

In a typical switch, each physical port consists of one or more queues for transmitting packets on the attached network. Multiple queues per port are often provided to give preference to certain packets over others based on user-defined criteria. When a packet is queued for transmission in a port, the rate at which it is serviced depends on how the queue is configured and possibly the amount of traffic present in the other queues of the port. If a delay is necessary, packets get held in the queue until the scheduler authorizes the queue for transmission. As queues become full, packets have no place to be held for transmission and get dropped by the switch.

QoS is a means of providing consistent, predictable data delivery by distinguishing between packets that have strict timing requirements from those that are more tolerant of delay. Packets with strict timing requirements are given "special treatment" in a QoS capable network. With this in mind, all elements of the network must be QoS-capable. The presence of at least one node which is not QoS-capable creates a deficiency in the network path and the performance of the entire packet flow is compromised.

To display the Quality of Service menu page, click **Quality of Service** in the tree view. The two types of QoS available are links on this menu page. These links are:

- Configuring Differentiated Services
- Class of Service
- Auto VoIP

Downloaded from www.Manualslib.com manuals search engine

Configuring Differentiated Services

DiffServ Overview

The QoS feature contains Differentiated Services (DiffServ) support that allows traffic to be classified into streams and given certain QoS treatment in accordance with defined per-hop behaviors.

Standard IP-based networks are designed to provide “best effort” data delivery service. “Best effort” service implies that the network delivers the data in a timely fashion, although there is no guarantee that it will. During times of congestion, packets may be delayed, sent sporadically, or dropped. For typical Internet applications, such as e-mail and file transfer, a slight degradation in service is acceptable and in many cases unnoticeable. Conversely, any degradation of service has undesirable effects on applications with strict timing requirements, such as voice or multimedia.

Defining DiffServ

To use DiffServ for QoS, the web pages accessible from the **Differentiated Services** menu page must first be used to define the following categories and their criteria:

1. Class: create classes and define class criteria
2. Policy: create policies, associate classes with policies, and define policy statements
3. Service: add a policy to an inbound interface

Packets are classified and processed based on defined criteria. The classification criteria is defined by a class. The processing is defined by a policy's attributes. Policy attributes may be defined on a per-class instance basis, and it is these attributes that are applied when a match occurs. A policy can contain multiples classes. When the policy is active, the actions taken depend on which class matches the packet.

Packet processing begins by testing the class match criteria for a packet. A policy is applied to a packet when a class match within that policy is found.

The **Differentiated Services** menu page contains links to the various Diffserv configuration and display features.

To display the page, click **Quality of Service > Differentiated Services** in the tree view. The Differentiated Services menu page contains links to the following features:

- Diffserv Configuration
- Class Configuration
- Class Criteria
- Policy Configuration
- Policy Class Definition
- Service Configuration
- Service Detailed Statistics

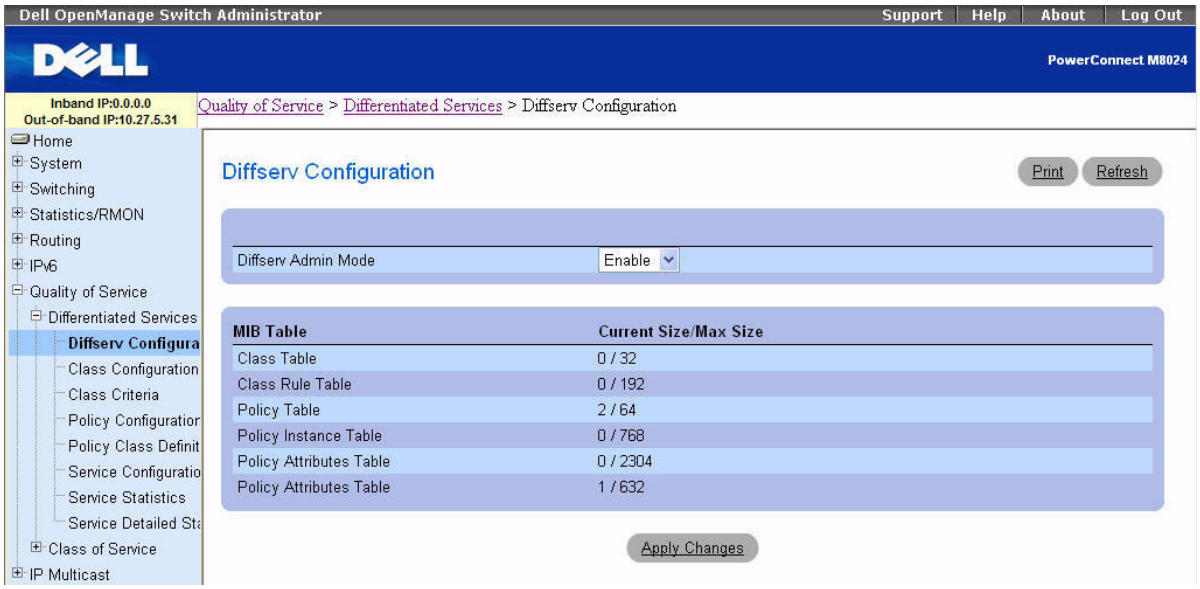
Downloaded from www.Manualslib.com manuals search engine

Diffserv Configuration

Use the **Diffserv Configuration** page to display DiffServ General Status Group information, which includes the current administrative mode setting as well as the current and maximum number of rows in each of the main DiffServ private MIB tables.

To display the page, click **Quality of Service > Differentiated Services > Diffserv Configuration** in the tree view.

Figure 11-1. Diffserv Configuration



The **Diffserv Configuration** page contains the following fields:

Diffserv Admin Mode — Turns admin mode on and off. While disabled, the DiffServ configuration is retained and can be changed, but it is not active. While enabled, Differentiated Services are active.

MIB Table

- **Class Table** — Displays the current and maximum number of rows of the class table.
- **Class Rule Table** — Displays the current and maximum number of rows of the class rule table.
- **Policy Table** — Displays the current and maximum number of rows of the policy table.
- **Policy Instance Table** — Displays the current and maximum number of rows of the policy instance table.
- **Policy Attributes Table** — Displays the current and maximum number of rows of the policy attributes table.
- **Service Table** — Displays the current and maximum number of rows of the service table.

Downloaded from www.Manualslib.com manuals search engine

Changing Diffserv Admin Mode

1. Open the **Diffserv Configuration** page.
2. Turn **Diffserv Admin Mode** on or off by selecting Enable or Disable from the drop-down menu.
3. Click **Apply Changes**.

   The Diffserv Admin Mode is changed, and the device is updated.

Displaying MIB Tables Using the CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide:*

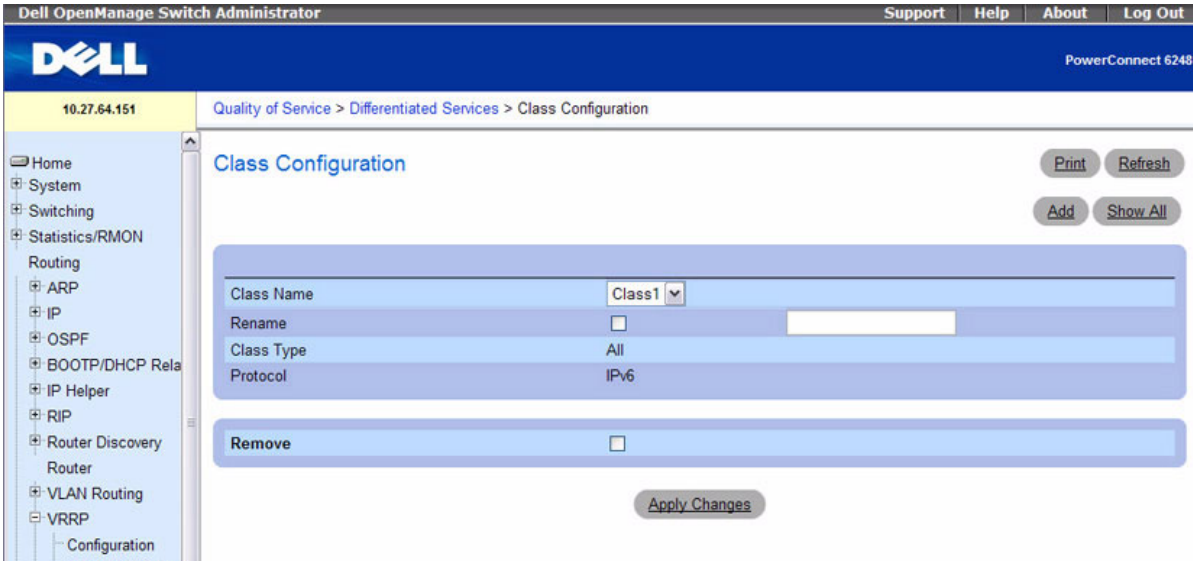
- QoS Commands

Class Configuration

Use the **Diffserv Class Configuration** page to add a new Diffserv class name, or to rename or delete an existing class.

To display the page, click **Quality of Service > Differentiated Services > Class Configuration** in the tree view.

Figure 11-2. Diffserv Class Configuration



The **Diffserv Class Configuration** page contains the following fields:

- **Class Name** — Selects a class name to rename or delete. Click **Add** to set up a new class name.
- **Rename** — Renames the class displayed when the box is checked and a new name is entered.
- **Class Type** — Lists the class types. Currently the hardware supports only the **Class Type** value **All**.

Downloaded from www.Manualslib.com manuals search engine

– All — All the various match criteria defined for the class should be satisfied for a packet match. **All** signifies the logical **AND** of all the match criteria.

- **Protocol** — Indicates how to interpret Layer 3. This field displays the types of packets supported by DiffServ. The Layer 3 Protocol option is available only when you select Class Type. Options are:
  – **IPv4** — A class where the match criteria is based on fields in an IPv4 packet.
  – **IPv6** — A class where the match criteria is based on fields in an IPv6 packet.

The protocol is chosen on the **Add DiffServ Class** page. See "Adding a DiffServ Class" on page 625.

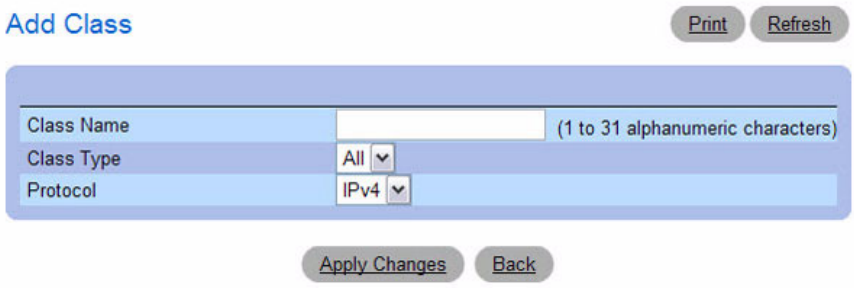
- **Remove** — Deletes the displayed class name when checked and **Apply Changes** is clicked.

Adding a DiffServ Class

1. Open the **Diffserv Class Configuration** page.
2. Click **Add**.

   The **Add DiffServ Class** page displays

Figure 11-3. Add DiffServ Class



Enter a name for the class and select the protocol to use for class match criteria.

3. Click **Apply Changes**.

   The new class is added and the device is updated.

Adding a Class Configuration Using the CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide:*

- QoS Commands

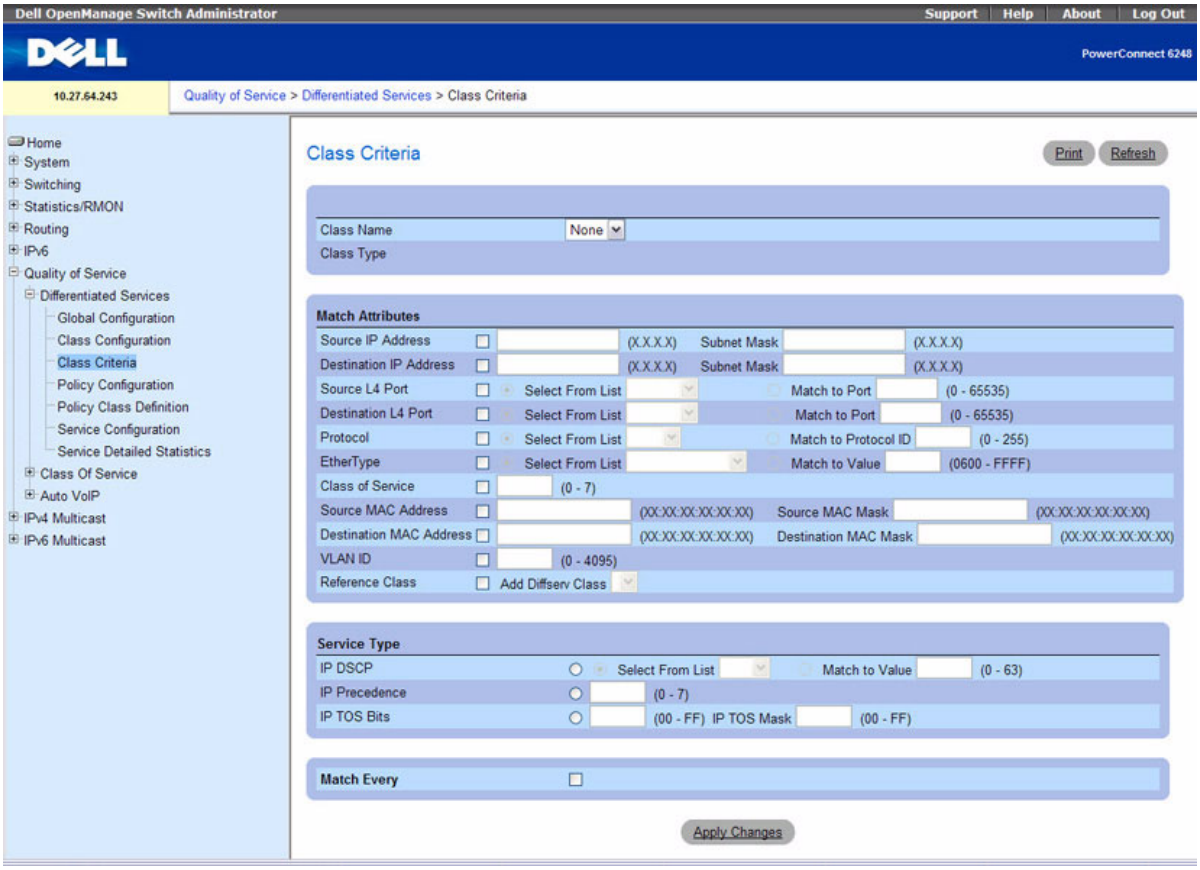
Downloaded from www.Manualslib.com manuals search engine

Class Criteria

Use the **Diffserv Class Criteria** page to define the criteria to associate with a DiffServ class. As packets are received, these DiffServ classes are used to prioritize packets.

To display the page, click **Quality of Service > Differentiated Services > Class Criteria** in the tree view.

Figure 11-4. Diffserv Class Criteria IPv4



The **Diffserv Class Criteria** page contains the following fields:

- **Class Name** — Selects the class name for which you are specifying criteria.
- **Class Type** — Displays the class type. The only configurable class type supported is **All**.

Downloaded from www.Manualslib.com manuals search engine

Match Attributes (IPv4)

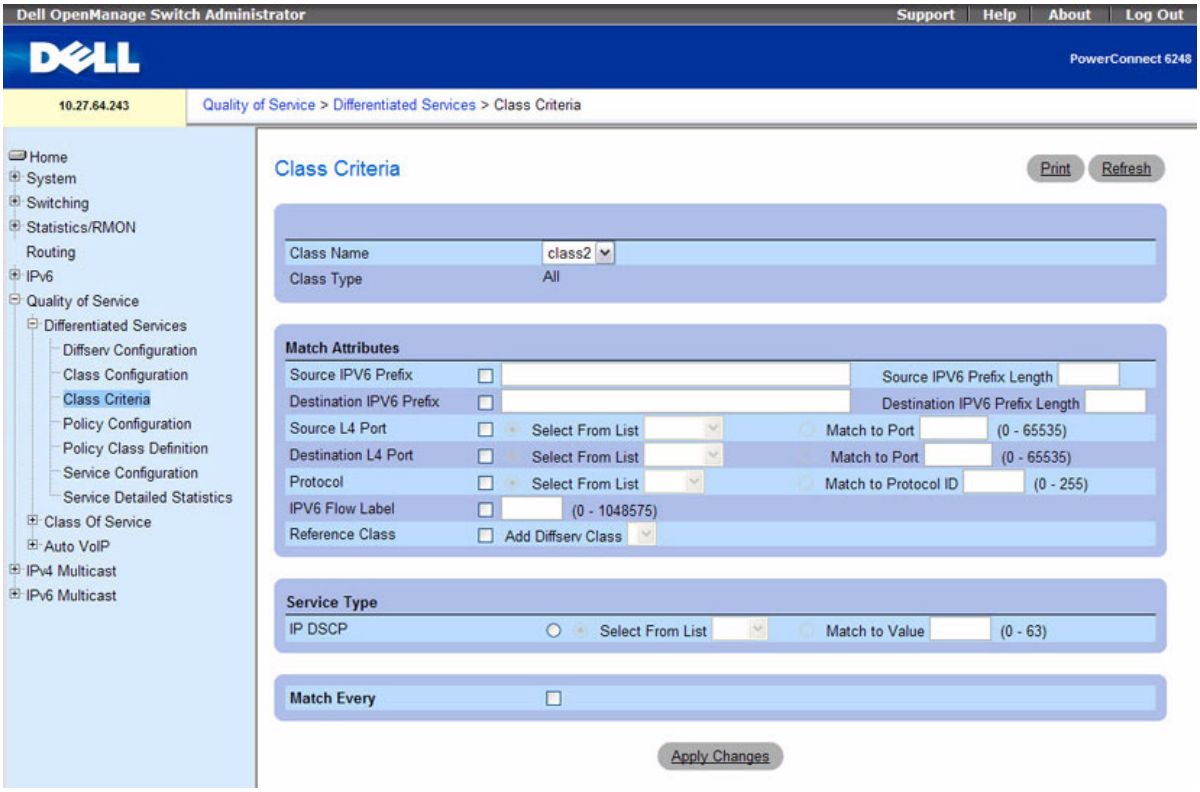
Use the following fields to match IPv4 packets to a class. Click the check box for each field to be used as a criterion for a class, and enter data in the related field. You can have multiple match criteria in a class. The logic is a Boolean "logical-and" for this criteria.

- **Source IP Address** — Requires a packet's source port IP address to match the address listed here.
- **Subnet Mask** — The subnet mask of the source IP address. This field is required when **Source IP Address** is checked.
- **Destination IP Address** — Requires a packet's destination port IP address to match the address listed here.
- **Subnet Mask** — The subnet mask of the destination IP address. This field is required when **Destination IP Address** is checked.
- **Source L4 Port**— Requires a packet's TCP/UDP source port to match the port listed here. Select one of the following options:
  - **Select From List** — Click to select from a list of well known source ports to which packets are matched.
  - **Match to Port** — Click to add a user-defined Port ID to which packets are matched. Range is 0-65535.
- **Destination L4 Port** — Requires a packet's TCP/UDP destination port to match the port listed here. Select one of the following:
  - **Select From List** — Select from a list of well known destination ports to which packets are matched.
  - **Match to Port** — Click to add a user-defined Port ID to which packets are matched. Range is 0-65535.
- **Protocol** — Requires a packet's protocol to match the protocol listed here. Select one of the following:
  - **Select from List** — Select from the drop-down list of protocols.
  - **Match to Protocol ID** — Enter a protocol ID to which packets are matched. Range is 0-255.
- **EtherType** — Requires a frames' Ethertype to match the Ethertype listed here. Select one of the following:
  - **Select from List** — Select from the drop-down list of EtherTypes.
  - **Match to Value** — Enter an Ethertype ID to which packets are matched. Range is 0600-FFFF.
- **Class of Service** — Requires a packet's Class of Service (CoS) for incoming packets to match the CoS entered here. Range is 0-7.
- **Source MAC Address** — Requires a packet's Source MAC Address for incoming packets to match the address entered here.

Downloaded from www.Manualslib.com manuals search engine

- **Source MAC Mask** — Specifies the Source MAC address wildcard mask. Wild card masks determine which bits are used and which bits are ignored. A wild card mask of 00.00.00.00.00.00 indicates that no bit is important. A wildcard of FF:FF:FF:FF:FF:FF indicates that all bits are important. This field is required when **Source MAC Address** is checked.
- **Destination MAC Address** — Requires a packet's Destination MAC Address for incoming packets to match the address entered here.
- **Destination MAC Mask** — Specifies the Destination MAC address wildcard mask. Wild card masks determine which bits are used and which bits are ignored. A wild card mask of 00.00.00.00.00.00 indicates that no bit is important. A wildcard of FF:FF:FF:FF:FF:FF indicates that all bits are important. This field is required when **Destination MAC Address** is checked.
- **VLAN ID** — Requires a packet's VLAN ID for incoming packets to match the VLAN ID entered here. Range is 0-4095.
- **Reference Class** — Selects a class to start referencing for criteria. Select the **Add Diffserv Class** check box, then select a previously configured Diffserv class from the related drop-down menu.

Figure 11-5. Diffserv Class Criteria IPv6



Downloaded from www.Manualslib.com manuals search engine

Match Attributes (IPv6)

Use the following fields to match IPv6 packets to a class. For other fields not listed here, see the description in "Match Attributes (IPv4)" on page 627. Click the check box for each field to be used as a criterion for a class, and enter data in the related field. You can have multiple match criteria in a class. The logic is a Boolean “logical-and” for this criteria.

- **Source IPv6 Prefix** — Requires a packet’s source port IPv6 address to match the address listed here. Enter the address in the format: aaaa:aaaa:aaaa:aaaa.
- **Source IPv6 Prefix Length** — Prefix Length can be entered in the range of 0-128.
- **Destination IPv6 Prefix** — Requires a packet’s destination port IPv6 address to match the address listed here. Enter the address in the format: aaaa:aaaa:aaaa:aaaa.
- **Destination IPv6 Prefix Length** — Prefix Length can be entered in the range of 0 to 128.
- **IPv6 Flow Label** — Flow label is a 20-bit number that is unique to an IPv6 packet, used by end stations to signify quality-of-service handling in routers. The flow label of the incoming packet must match this value. Range is 0-1048575.

Service Type Criteria

Click to select one of the following three Match fields to use in matching packets to class criteria:

- **IP DSCP** — Matches the packet’s DSCP to the class criteria’s when selected. Either select the DSCP type from the drop-down menu or enter a DSCP value to match. Valid range is 0-63.
- **Match Every** — Requires a packet to match every criterion when **Match Every** is checked.

Configuring Class Criteria with CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide:*

- QoS Commands

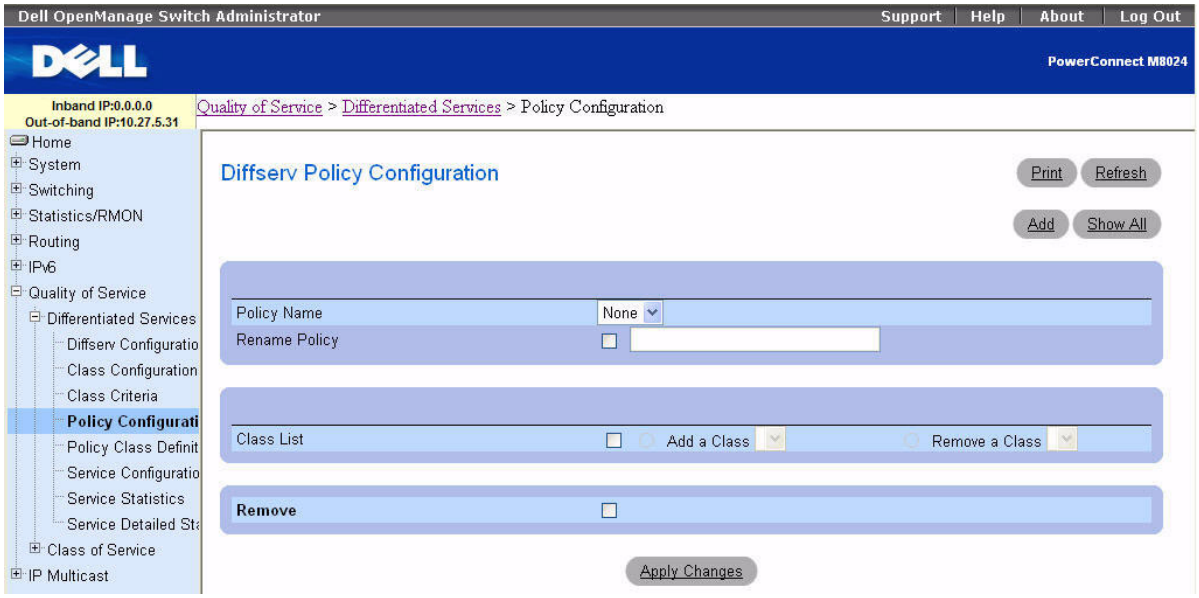
Downloaded from www.Manualslib.com manuals search engine

Policy Configuration

Use the **Diffserv Policy Configuration** page to associate a collection of classes with one or more policy statements.

To display the page, click **Quality of Service > Differentiated Services > Policy Configuration** in the tree view.

Figure 11-6. Diffserv Policy Configuration



The **Diffserv Policy Configuration** page contains the following fields:

- **Policy Name** — Selects the policy name to be associated with the class(es).
- **Rename Policy** — Renames a policy when box is checked, a new name is entered, and **Apply Changes** is clicked.
- **Class List** — Configures class association for the policy.
  - **Add a Class** — Associates the class selected in the drop-down menu to a policy.
  - **Remove a Class** — Removes the selected class from the policy.
- **Remove** — Deletes the selected policy name from the device.

Associating a Class to a Policy or Removing the Association

1. Open the **Diffserv Policy Configuration** page.
2. Select the **Policy Name** to associate with the class.
3. In **Class List** field, select the check box, then click the **Add a Class** or **Remove a Class** radio button and select the **class** from the related drop down menu

Downloaded from www.Manualslib.com manuals search engine

Use **Add a Class** to associate a class with this policy. Use **Remove a Class** to remove the class from this policy.

4. Select the class to be affected from the relevant drop-down menu.
5. Click **Apply Changes**.

   The modified policy is saved, and the device is updated.

Renaming a Policy

1. Open the **Diffserv Policy Configuration** page.
2. Select the **Policy Name** to be renamed.
3. Rename policy by checking **Rename Policy** and entering the new name in the adjacent field.

   The modified policy name is saved, and the device is updated.

Adding a New Policy Name

1. Open the **Diffserv Policy Configuration** page.
2. Click **Add**.

   The **Add Diffserv Policy** page displays.

Figure 11-7. Add Diffserv Policy

3. Enter the new **Policy Name**.
4. Click **Apply Changes**.

   The new policy is saved, and the device is updated.

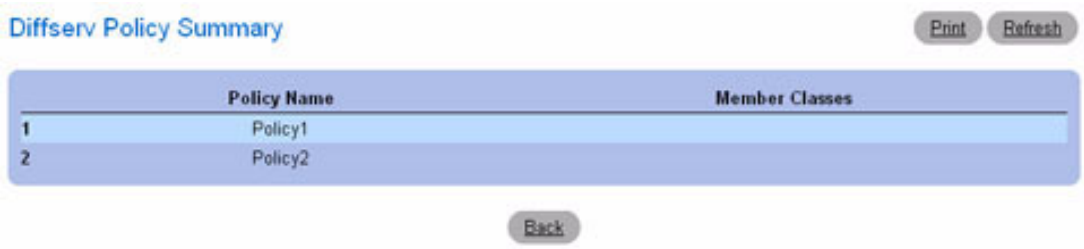
Displaying the Policy Summary

1. Open the **Policy Configuration** page.
2. Click **Show All**.

   The **Diffserv Policy Summary** page displays all policy names, their policy types, and their member classes.

Downloaded from www.Manualslib.com manuals search engine

Figure 11-8. Diffserv Policy Summary



Removing a Policy Configuration

1. Open the **Diffserv Policy Configuration** page.
2. Select the policy name to be deleted from the **Policy Name** drop-down menu.
3. Check the **Remove** check box.
4. Click **Apply Changes**.

   The associated policy configuration is removed, and the device is updated.

Defining Policy Configurations Using the CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide:*

- QoS Commands

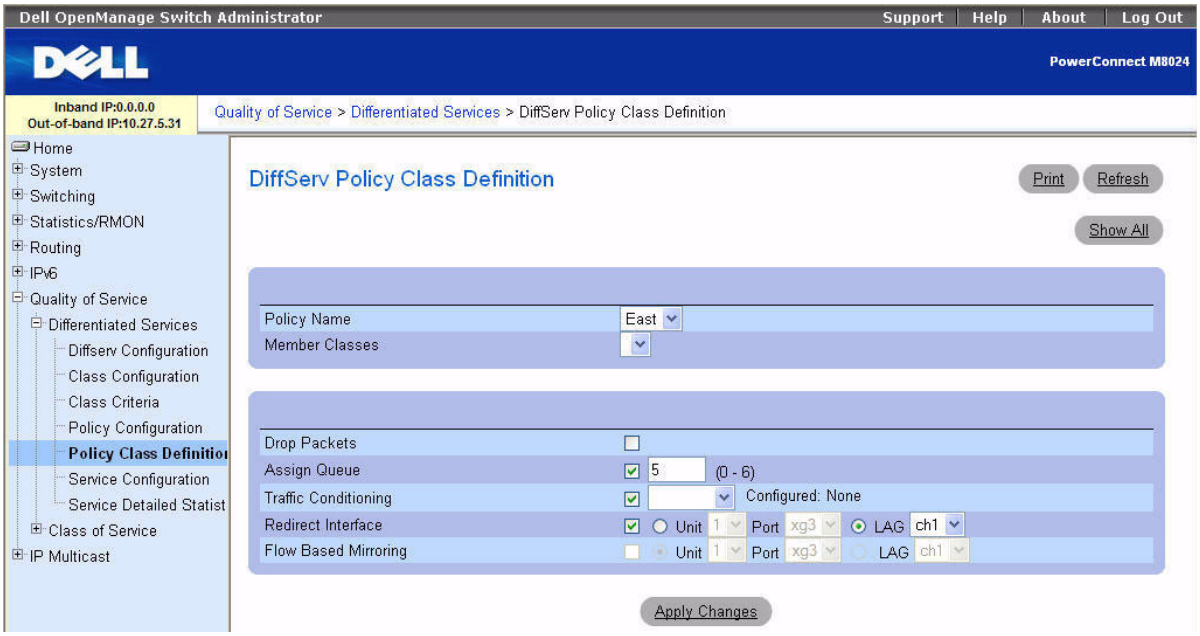
Downloaded from www.Manualslib.com manuals search engine

Policy Class Definition

Use the **Diffserv Policy Class Definition** page to associate a class to a policy, and to define attributes for that policy-class instance.

To display the page, click **Quality of Service > Differentiated Services > Policy Class Definition** in the tree view.

Figure 11-9. Diffserv Policy Class Definition



The **Diffserv Policy Class Definition** page contains the following fields:

- **Policy Name** — Selects the policy to associate with a member class from a drop-down menu.
- **Member Classes** — Selects the member class to associate with this policy name from a drop-down menu.
- **Drop Packets** — Select this field to drop packets for this policy-class.
- **Assign Queue** — Assigns the packets of this policy-class to a queue. The valid range is 0–6.
- **Traffic Conditioning** — Assigns a type of traffic conditioning when checked and a condition is selected from the drop-down menu. This field affects how traffic that matches this policy-class is treated. Choose from **None**, **Marking**, and **Policing**. When **Marking** or **Policing** is selected, the screen changes to display related fields.
  - **None**: Specifies no traffic conditioning occurs during packet processing. This is the default.
  - **Marking**: Allows you to mark one of the following fields in the packet: IP DSCP, IP Precedence, or Class of Service. For information on the fields that display when **Marking** is selected, see "Packet Marking Traffic Condition."

Downloaded from www.Manualslib.com manuals search engine

– **Policing**: Allows you to configure how policing is performed, as well as configure what happens to packets that are considered conforming and non-conforming. For more information on the fields that display when **Policing** is selected, see "Policing Traffic Condition."

- **Redirect Interface** — Displays whether Redirect Interface applies to this policy-class, and specifies the interface or LAG used.
- **Flow Based Mirroring** — Displays whether Flow Based Mirroring applies to this policy-class, and specifies the interface or LAG used.

Defining a Policy-Class Instance

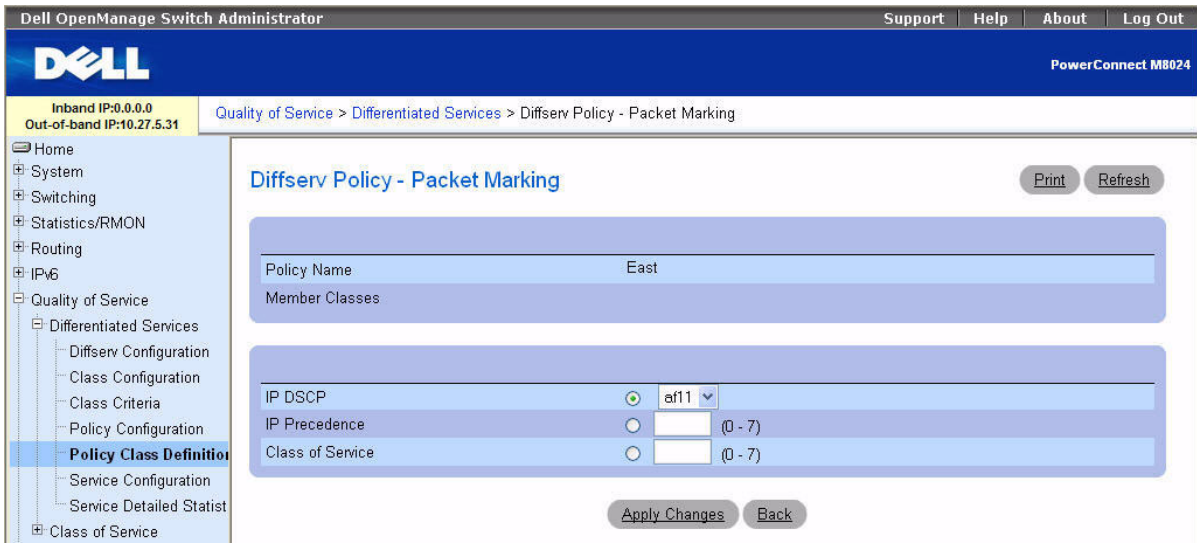
1. Open the **Diffserv Policy Class Definition** page.
2. Select a policy and member class to associate.
3. Specify attributes to apply to this policy-class instance using the remaining fields on the page.
4. Click **Apply Changes**.

   The policy-class is defined, and the device is updated.

Packet Marking Traffic Condition

When **Marking** is chosen as the **Traffic Condition**, the following Packet Marking page displays.

Figure 11-10. Policy Class Definition - Packet Marking



The **Diffserv Policy - Packet Marking** page contains the following fields:

- **Policy Name**— Displays the policy associated with a member class.
- **Member Classes** — Displays the member class associated with this policy name.

You have the option of marking one of the following fields in the packet:

Downloaded from www.Manualslib.com manuals search engine

- **IP DSCP** — Selects the IP DSCP to mark. Select from the drop down menu or enter directly in the User Value field.
- **IP Precedence** — Selects the specified IP Precedence queue number to mark.

Class of Service — Selects the specified Class of Service queue number to mark.

Configuring Packet Marking for a Policy Class Instance

1. Select **Marking** from the **Traffic Conditioning** drop-down menu on the **Diffserv Policy Class Definition** page.

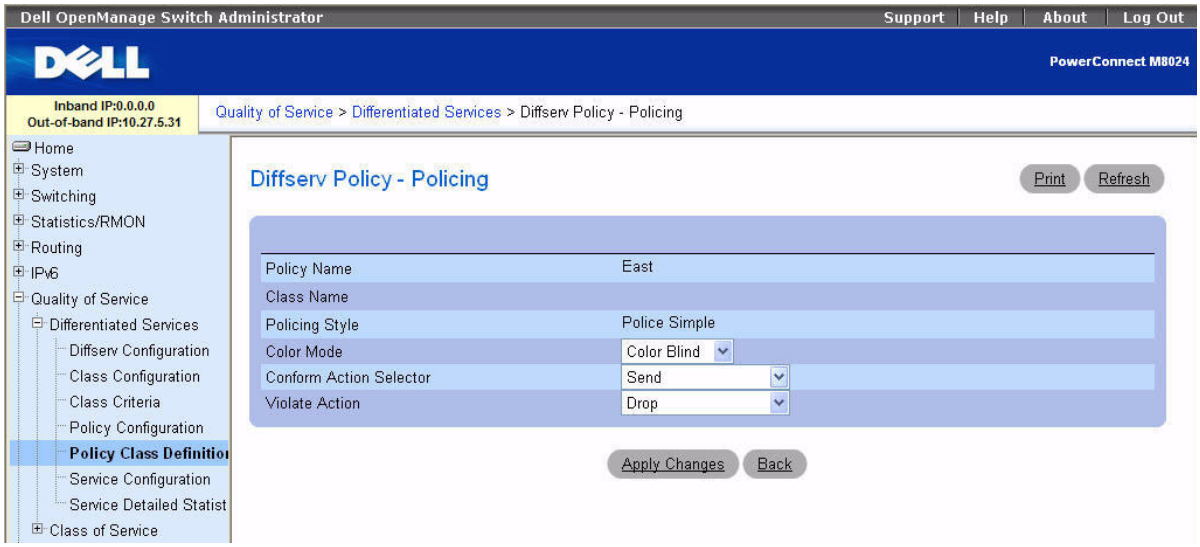
   The **Packet Marking** page displays.
2. Select IP DSCP, IP Precedence, or Class of Service to mark for this policy-class.
3. Select or enter a value for this field.
4. Click **Apply Changes**.

   The policy-class is defined, and the device is updated.

Policing Traffic Condition

When **Policing** is chosen as the **Traffic Condition**, the following **Diffserv Policy - Policing** page displays.

Figure 11-11. Policy Class Definition - Policing



The **Diffserv Policy - Policing** page contains the following fields:

- **Policy Name** — Displays the policy for which policing is being configured.
- **Class Name** — Displays the member class associated with this policy name.
- **Policing Style** — Displays the style of policing being used.

Downloaded from www.Manualslib.com manuals search engine

- **Color Mode** — Selects the type of color policing used. Choose Color Blind or Color Aware from the drop-down menu.
- **Conform Action Selector** — Selects what happens to packets that are considered conforming (below the police rate). Options are Send, Drop, Mark CoS, Mark IP DSCP, Mark IP Precedence.
- **Violate Action** — Selects what happens to packets that are considered non-conforming (above the police rate). Options are Send, Drop, Mark CoS, Mark IP DSCP, Mark IP Precedence.

Configuring Policing for a Policy-Class Instance

1. Select **Policing** from the **Traffic Conditioning** drop-down menu on the **Diffserv Policy Class Definition** page.

   The **Diffserv Policy - Policing** page displays.
2. Check to select one or more policing criteria to use for this policy-class.
3. Select or enter a value for each field selected.
4. Click **Apply Changes**.

   The following **Policy Rate Configuration** page displays.

Figure 11-12. Policy Rate Configuration

5. Enter the desired criteria values for Committed Rate and/or Committed Burst Size.
6. Click **Apply Changes.**

   Policing is configured for the specified policy-class instance, and the device is updated.

Defining Policy Classes Using the CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide:*

- QoS Commands

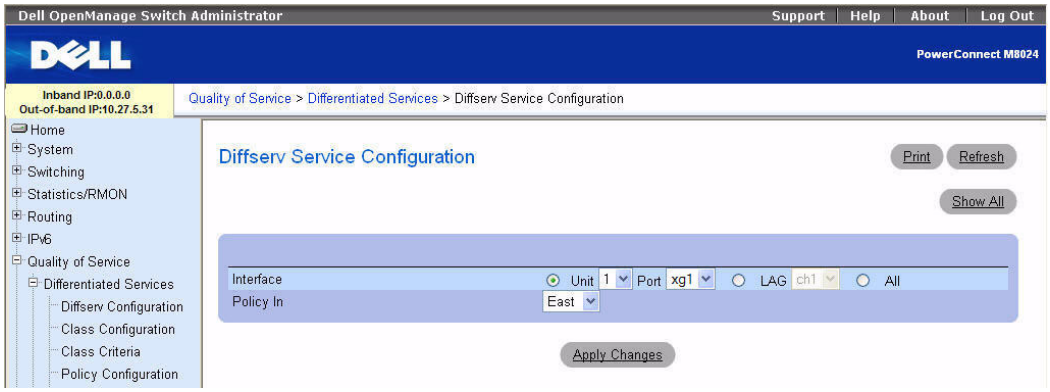
Downloaded from www.Manualslib.com manuals search engine

Service Configuration

Use the **Diffserv Service Configuration** page to activate a policy on a port.

To display the page, click **Quality of Service > Differentiated Services > Service Configuration** in the tree view.

Figure 11-13. Diffserv Service Configuration



The **Diffserv Service Configuration** page contains the following fields:

- **Interface** — Selects the interface (Unit/Port, LAG, or All) to be affected from drop-down menus.
- **Policy In** — Selects the policy to be associated with the port from a drop-down menu.

Activating a Policy on a Port

1. Open the **Diffserv Service Configuration** page.
2. Select the interface from the drop-down menus.
3. Select the policy from the drop-down menu.
4. Click **Apply Changes**.

   The policy is activated on the interface, and the device is updated.

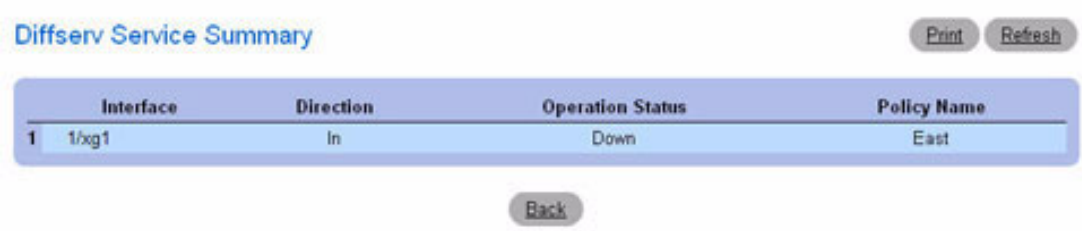
Displaying Diffserv Service Summary

1. Open the **Diffserv Service Configuration** page.
2. Click **Show All**.

   The Diffserv Service Summary page displays.

Downloaded from www.Manualslib.com manuals search engine

Figure 11-14. Diffserv Service Summary



Assigning a Policy to a Port Using the CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide:*

- QoS Commands

Service Detailed Statistics

Use the **Diffserv Service Detailed Statistics** page to display packet details for a particular port and class.

To display the page, click **Quality of Service > Differentiated Services > Service Detailed Statistics** in the tree view.

Figure 11-15. Diffserv Service Detailed Statistics

The **Diffserv Service Detailed Statistics** page contains the following fields:

- **Counter Mode Selector** — Type of statistics to display. Packets is the only available type.
- **Interface** — Selects the Unit and Port or LAG for which service statistics are to display.
- **Direction** — Selects the direction of packets for which service statistics are to display.

Downloaded from www.Manualslib.com manuals search engine

- **Policy Name** — Displays the policy associated with the selected interface.
- **Operational Status** — Displays whether the policy is active or not on this interface.
- **Member Classes** — Selects the member class for which octet statistics are to display.
- **Offered Packets** — Displays how many packets match the policy.
- **Discarded Packets** — Displays how many packets are dropped by the policy.

Displaying Service Statistics

1. Open the **Diffserv Service Detailed Statistics** page.
2. Complete the fields as needed.

   Packet statistics display for the specified interface, direction, and class.

Configuring Service Statistics Using the CLI Command

For information about the CLI command that performs this function, see the following chapter in the *CLI Reference Guide:*

- QoS Commands

Class of Service

The Class of Service (CoS) queueing feature lets you directly configure certain aspects of switch queueing. This provides the desired QoS behavior for different types of network traffic when the complexities of DiffServ are not required. The priority of a packet arriving at an interface can be used to steer the packet to the appropriate outbound CoS queue through a mapping table. CoS queue characteristics that affect queue mapping, such as minimum guaranteed bandwidth, transmission rate shaping, etc., are user-configurable at the queue (or port) level.

Seven queues per port are supported. Although the hardware supports eight queues, one queue is always reserved for internal use by the stacking subsystem.

To display the page, click **Quality of Service > Class of Service** in the tree view. The **Class of Service** menu page contains links to the following features:

- Mapping Table Configuration
- Interface Configuration
- Interface Queue Configuration

Downloaded from www.Manualslib.com manuals search engine

Mapping Table Configuration

Each port in the switch can be configured to trust one of the packet fields (802.1p, IP Precedence, or IP DSCP), or to not trust any packet's priority designation (untrusted mode). If the port is set to a trusted mode, it uses a mapping table appropriate for the trusted field being used. This mapping table indicates the CoS queue to which the packet should be forwarded on the appropriate egress port(s). Of course, the trusted field must exist in the packet for the mapping table to be of any use, so there are default actions performed when this is not the case. These actions involve directing the packet to a specific CoS level configured for the ingress port as a whole, based on the existing port default priority as mapped to a traffic class by the current 802.1p mapping table.

Alternatively, when a port is configured as untrusted, it does not trust any incoming packet priority designation and uses the port default priority value instead. All packets arriving at the ingress of an untrusted port are directed to a specific CoS queue on the appropriate egress port(s), in accordance with the configured default priority of the ingress port. This process is also used for cases where a trusted port mapping is unable to be honored, such as when a non-IP packet arrives at a port configured to trust the IP DSCP value.

Use the **Mapping Table Configuration** page to define how class of service is assigned to a packet.

To display the page, click **Quality of Service > Class of Service > Mapping Table Configuration** in the tree view.

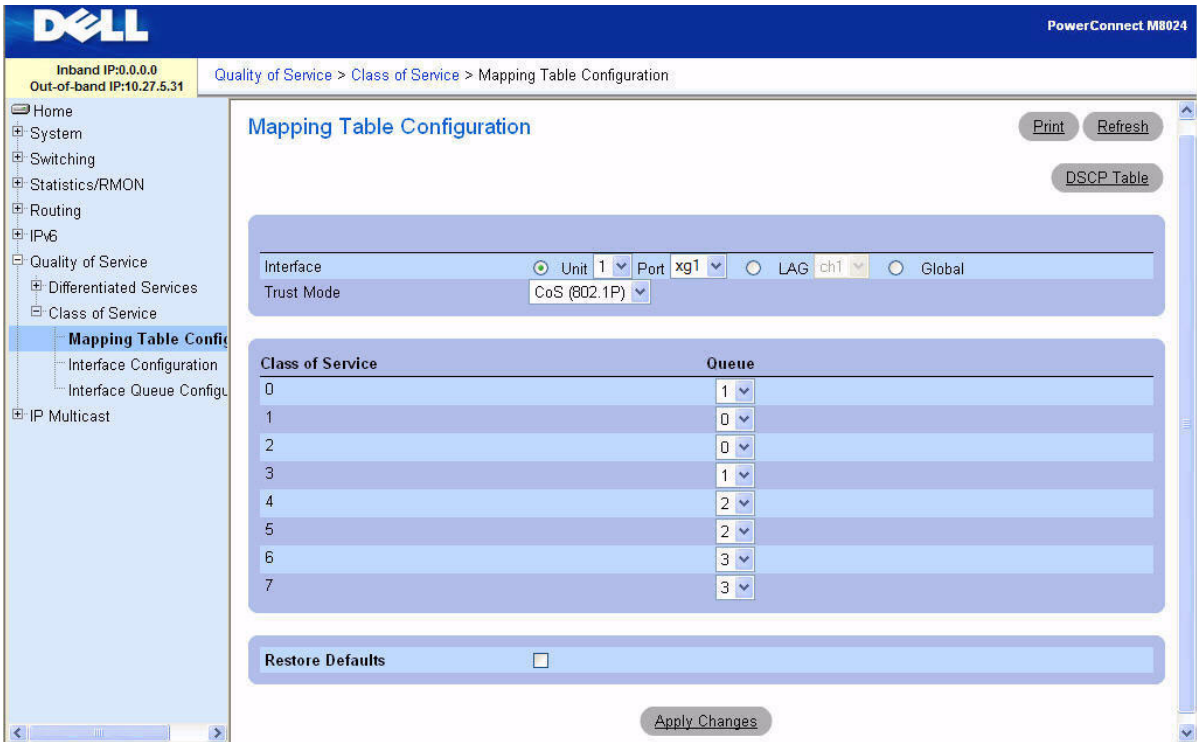
The Trust Mode selected on the **Mapping Table Configuration** page affects how the page displays and the fields accessible from the page. There are three trust modes available from here:

- Untrusted (None)
- CoS(802.1P)
- IP DSCP

CoS(802.1P) is the default mode, so this is the page that displays when **Mapping Table Configuration** is selected from the **Class of Service** menu page.

Downloaded from www.Manualslib.com manuals search engine

Figure 11-16. Mapping Table Configuration — CoS (802.1P)



CoS (802.1P) Trust Mode

The **CoS (802.1P) Mapping Table Configuration** page contains the following fields:

- **Interface** — Selects the interface to which the class of service configuration is applied. Select a unit and port or LAG, or select Global to apply the class of configuration to all the interfaces.
- **Trust Mode** — Selects the trust mode to apply. **CoS (802.1P)** is the default.
- **Class of Service** — Lists each class of service on a separate line, so a separate queue can be assigned to each class of service.
- **Queue** — Selects a queue for each **Class of Service** from the drop-down menu. Default queues are displayed initially.
- **Restore Defaults** — Restores default queue values when checked and **Apply Changes** is clicked.

Downloaded from www.Manualslib.com manuals search engine

Configuring CoS (802.1P) Trust Mode

1. Open the **Mapping Table Configuration** page.
2. Select the unit and port or LAG to be affected, or select Global to apply the settings to all interfaces.
3. Select a **Trust Mode**.
4. Select a **Queue** to associate with each **Class of Service**.
5. Click **Apply Changes**.

   Changes made are applied to the selected interfaces, and the device is updated.

Restoring Queue Defaults

1. Open the **Mapping Table Configuration** page.
2. Click the **Restore Defaults** check box.
3. Click **Apply Changes**.

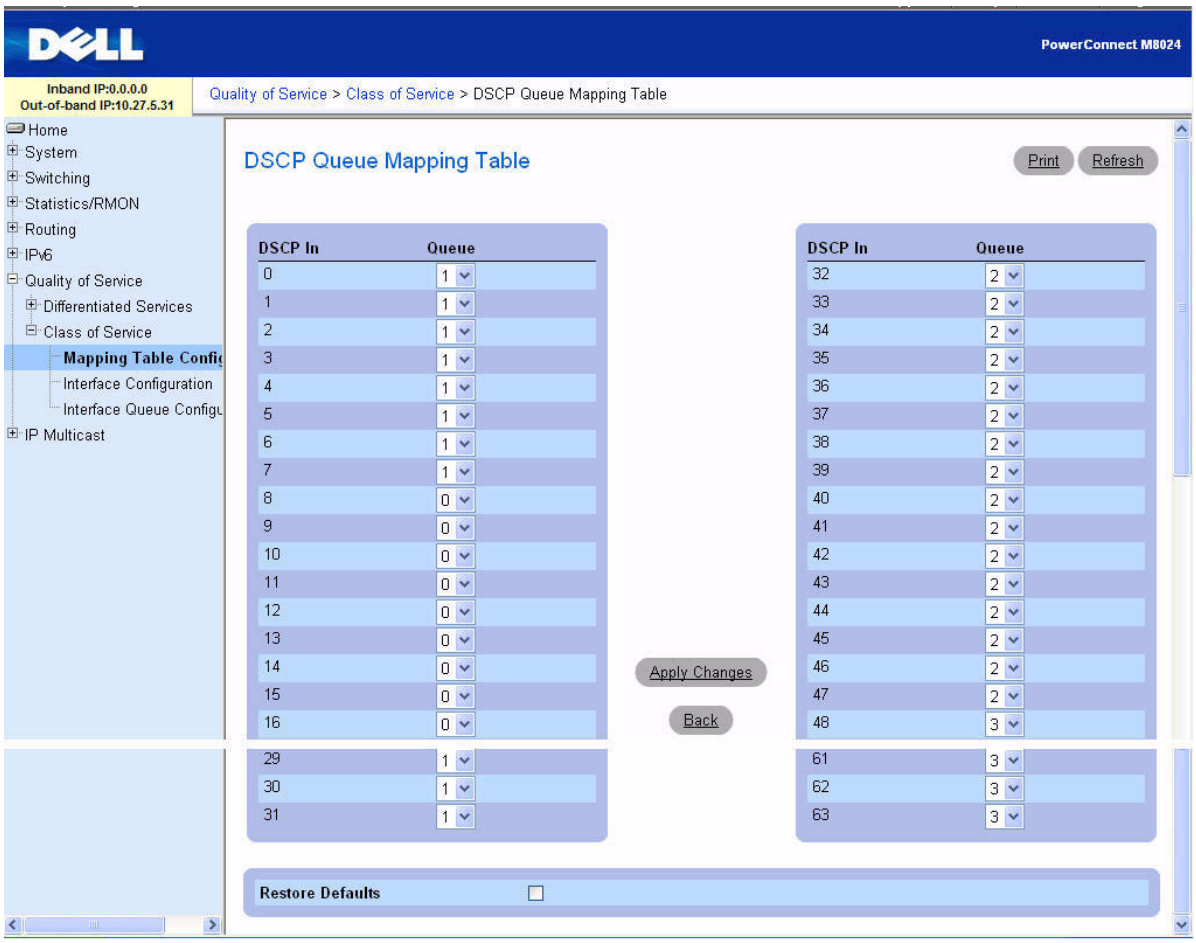
   Queues are returned to their defaults for each Class of Service, and the device is updated.

Downloaded from www.Manualslib.com manuals search engine

Configuring the IP DSCP Table

To access the **DSCP Queue Mapping Table**, click **Quality of Service > Class of Service > Mapping Table Configuration** in the tree view, and then click the DSCP Table link.

Figure 11-17. DSCP Queue Mapping Table



Downloaded from www.Manualslib.com manuals search engine

The **DSCP Queue Mapping Table** page contains the following fields:

- **DSCP In** — Check to select as a criterion, and enter which DiffServ Code Point in the packet to use. This field determines to which queue the packet is sent.
- **Queue ID** — Selects the queue to which the packet is sent.

Restoring Queue Defaults

1. Open the **DSCP Queue Mapping Table** page.
2. Click the **Restore Defaults** check box.
3. Click **Apply Changes**.

   Queue values are returned to their defaults, and the device is updated.

Mapping Table Configuration Using the CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide:*

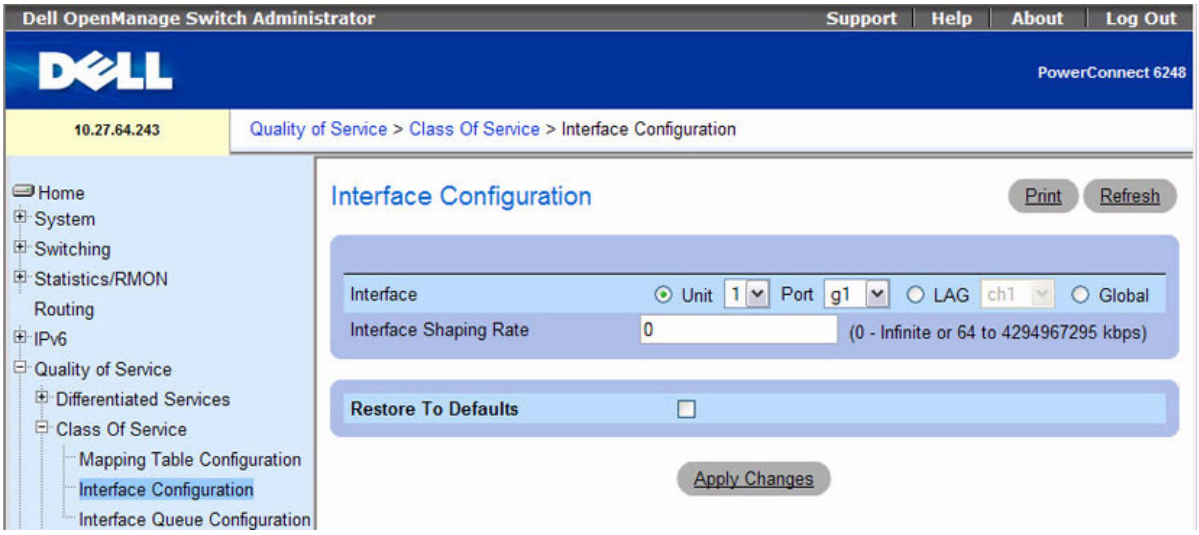
- QoS Commands

Interface Configuration

Use the **Interface Configuration** page to specify ports individually for CoS configuration and to apply an interface shaping rate to the selected ports.

To display the Interface Configuration page, click **Quality of Service > Class of Service > Interface Configuration** in the tree view.

Figure 11-18. Interface Configuration



Downloaded from www.Manualslib.com manuals search engine

The **Interface Configuration** page contains the following fields:

- **Interface** — Selects the interface to be affected by the **Interface Shaping Rate**. Select **Unit/Port**, or **LAG** to be affected from the drop-down menu. Select **Global** to specify all interfaces.
- **Interface Shaping Rate** — Sets the cap on how much traffic can leave a port. The specified value represents the maximum negotiated bandwidth in kilobit per second (Kbps). The range is 0 - Infinity or 64 to 4294967295 kbps.
- **Restore to Defaults** — Restores the default interface shaping rate to the selected interfaces when checked.

Defining Interface Configuration

1. Open the **Interface Configuration** page.
2. Select the unit and port or LAG to be affected, or select Global to apply the settings to all interfaces.
3. Enter an **Interface Shaping Rate** to apply to these ports.
4. Click **Apply Changes**.

   The new **Interface Shaping Rate** is applied to the selected interface(s) and the device is updated.

Restoring Default Shaping Rate

1. Open the **Interface Configuration** page.
2. Click the **Restore to Defaults** check box.
3. Click **Apply Changes**.

   All ports are restored to the default shaping rate, and the device is updated.

Defining Interface Configuration Using the CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide:*

- QoS Commands

Interface Queue Configuration

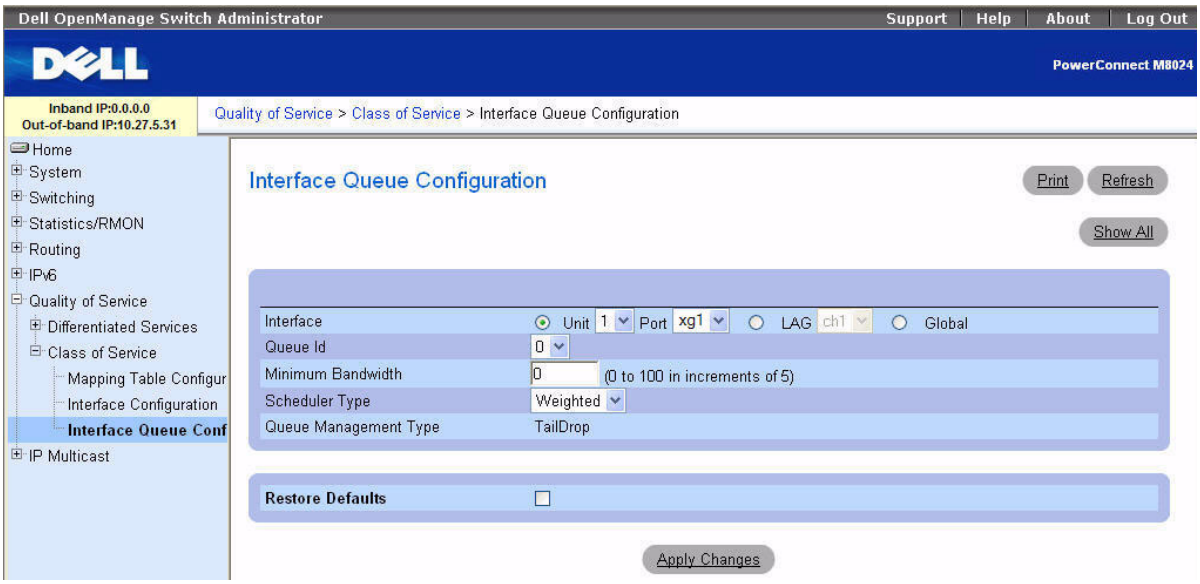
Use the **Interface Queue Configuration** page to define what a particular queue does by configuring switch egress queues. User-configurable parameters control the amount of bandwidth used by the queue, the queue depth during times of congestion, and the scheduling of packet transmission from the set of all queues on a port. Each port has its own CoS queue-related configuration.

The configuration process is simplified by allowing each CoS queue parameter to be configured globally or per-port. A global configuration change is automatically applied to all ports in the system.

To display the **Interface Queue Configuration** page, click **Quality of Service > Class of Service > Interface Queue Configuration** in the tree view.

Downloaded from www.Manualslib.com manuals search engine

Figure 11-19. Interface Queue Configuration



The **Interface Queue Configuration** page contains the following fields:

- **Interface** — Specifies the **Interface** (Unit/Port, LAG, or Global) that's being configured.
- **Queue ID** — Selects the queue to be configured from the drop-down menu.
- **Minimum Bandwidth** — Selects a percentage of the maximum negotiated bandwidth for the port. Specify a percentage from 0 to 100, in increments of 5.
- **Scheduler Type** — Selects the type of queue processing from the drop-down menu. Options are **Weighted** and **Strict**. Defining on a per-queue basis allows the user to create the desired service characteristics for different types of traffic.
  - **Weighted** — Weighted round robin associates a weight to each queue. This is the default.
  - **Strict** — Strict priority services traffic with the highest priority on a queue first.
- **Queue Management Type** — Displays the type of packet management used for all packets, which is Taildrop. All packets on a queue are safe until congestion occurs. At this point, any additional packets queued are dropped.

Configuring an Interface Queue

1. Open the **Interface Queue Configuration** page.
2. Select the port to be affected from the **Interface Unit** and **Port** drop-down menus.
3. Use the remaining fields to configure the queue and its settings for this port.
4. Click **Apply Changes**.

   The queue is configured, and the device is updated.

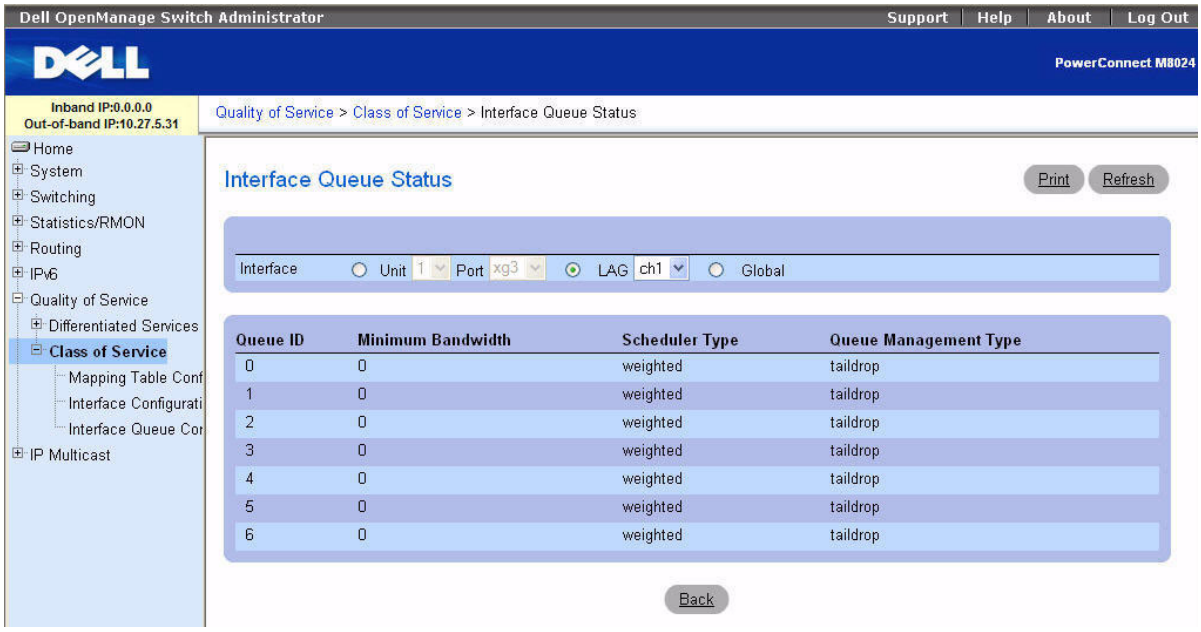
Downloaded from www.Manualslib.com manuals search engine

Displaying Interface Queue Settings

1. Open the **Interface Queue Configuration** page.
2. Click **Show All**.

   The **Interface Queue Status** page displays.
3. Select **Unit / Port**, **LAG**, or **Global**.

Figure 11-20. Interface Queue Status



Configuring an Interface Queue Using the CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide:*

- QoS Commands

Downloaded from www.Manualslib.com manuals search engine

Auto VoIP

Voice over Internet Protocol (VoIP) allows you to make telephone calls using a computer network over a data network like the Internet. With the increased prominence of delay-sensitive applications (voice, video, and other multimedia applications) deployed in networks today, proper QoS configuration will ensure high-quality application performance. The Auto VoIP feature is intended to provide an easy classification mechanism for voice packets so that they can be prioritized above data packets in order to provide better QoS.

The Auto VoIP feature explicitly matches VoIP streams in Ethernet switches and provides them with a better class of service than ordinary traffic. If you enable the Auto VoIP feature on an interface, the interface scans incoming traffic for the following call-control protocols:

- Session Initiation Protocol (SIP)
- H.323
- Skinny Client Control Protocol (SCCP)

When a call-control protocol is detected the switch assigns the traffic in that session to the highest CoS queue, which is generally used for time-sensitive traffic.

To display the page, click **Quality of Service > Auto VoIP** in the tree view. The **Auto VoIP** menu page contains links to the following pages:

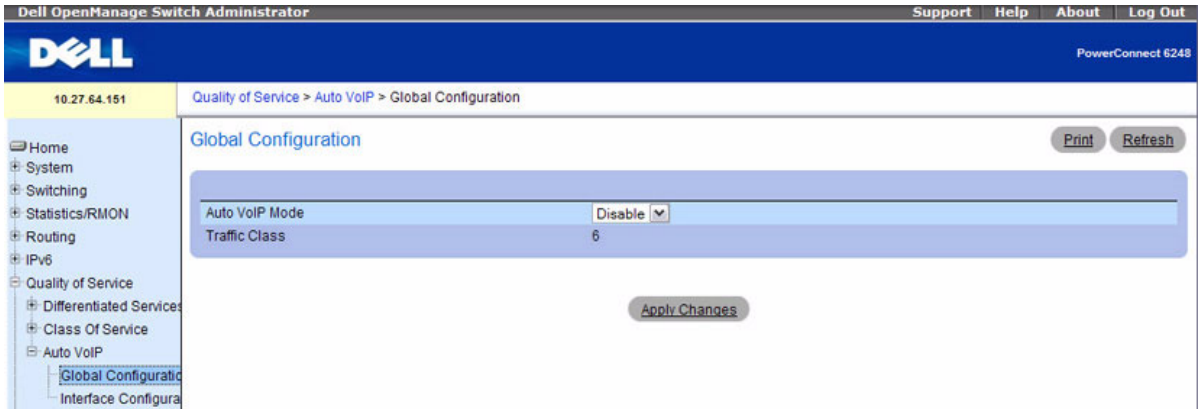
- Auto VoIP Global Configuration
- Auto VoIP Interface Configuration

Auto VoIP Global Configuration

Use the Auto VoIP Configuration page to configure the Auto VoIP settings on the switch.

To display the Auto VoIP Configuration page, click **Quality of Service > Auto VoIP > Global Configuration** in the navigation menu.

Figure 11-21. Auto VoIP Configuration



Downloaded from www.Manualslib.com manuals search engine

The **Auto VoIP Configuration** page contains the following fields:

- **Auto VoIP Mode** — Enables or Disables Auto VoIP mode. The default is Disable.
- **Traffic Class** —Displays the traffic class used for VoIP traffic.

Configuring Auto VoIP Using the CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide:*

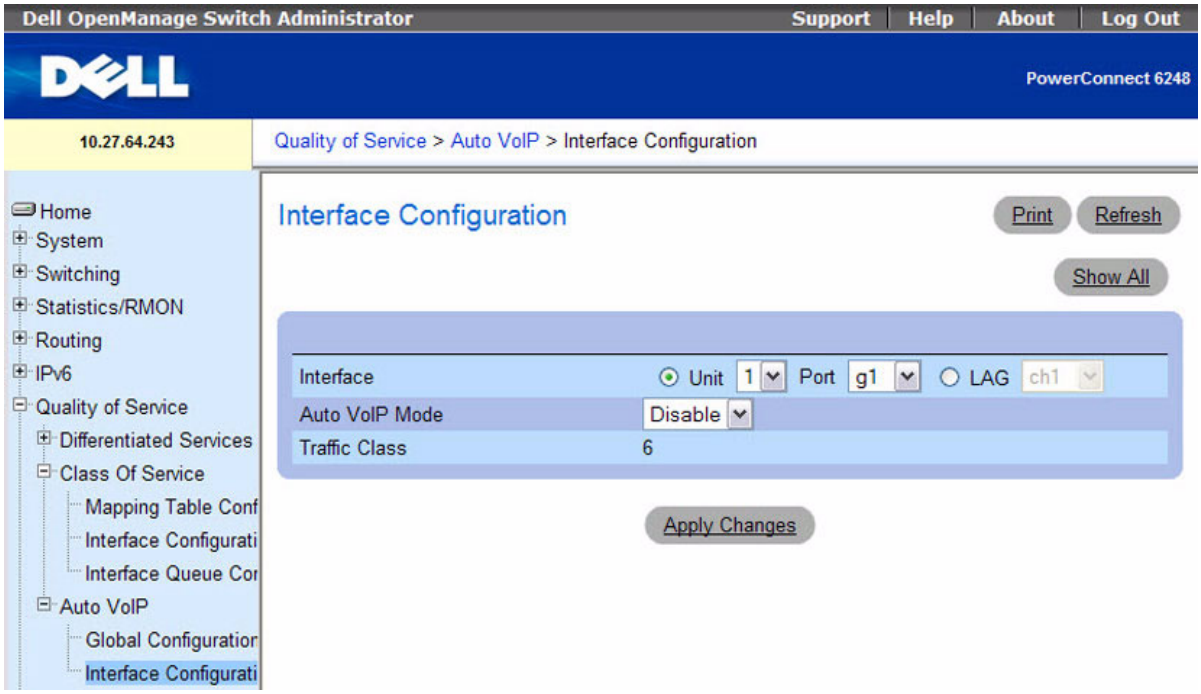
- QoS Commands

Auto VoIP Interface Configuration

Use the Auto VoIP **Interface Configuration** page to configure the Auto VoIP settings for each interface.

To display the Auto VoIP Configuration page, click **Quality of Service > Auto VoIP > Interface Configuration** in the navigation menu.

Figure 11-22. Auto VoIP Interface Configuration



The **Auto VoIP Interface Configuration** page contains the following fields:

- **Interface** — Lists the interfaces, Unit and Port or LAG, on which Auto VoIP can be configured.
- **Auto VoIP Mode** — Use the mode setting to either Enable or Disable the Auto VoIP mode on the selected interface. The default is Disable.
- **Traffic Class** —Displays the traffic class used for VoIP traffic.

Downloaded from www.Manualslib.com manuals search engine

Viewing the Auto VoIP Summary Table

1. Open the **Auto VoIP Interface Configuration** page.
2. Click **Show All**.

   The **Auto VoIP Summary** page opens.

Figure 11-23. Auto VoIP Summary

Auto VoIP Summary

Print Refresh

Interface	Auto VoIP Mode	Traffic Class
1/g1	Disable	6
1/g2	Disable	6
1/g3	Disable	6
1/g4	Disable	6
1/g5	Disable	6
1/g6	Disable	6
1/g7	Disable	6
1/g8	Disable	6
1/g9	Disable	6
1/g10	Disable	6
1/g11	Disable	6

Configuring Auto VoIP Using the CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide:*

- QoS Commands

Downloaded from www.Manualslib.com manuals search engine

12

Configuring IP Multicast

Overview

This chapter describes how to configure multicast features on the PowerConnect M6220/M6348/M8024.

Multicast protocols are used to deliver Multicast packets from one source to multi receivers. They facilitate better bandwidth utilization, less host and router processing, making them ideal for usage in applications like video or audio conferencing, Whiteboard tools, stock distribution tickers etc.

Multicast applications send one copy of a packet, and address it to a group of receivers (Multicast Group Address) rather than to a single receiver (unicast address). Multicast depends on the network to forward the packets to only those networks and hosts that need to receive them.

Multicast capable/enabled routers forward multicast packets based on the routes in the Multicast Routing Information Base (MRIB). These routes are created in the MRIB during the process of building multicast distribution trees by the Multicast Protocols running on the router. Different IP Multicast routing protocols use different techniques to construct these multicast distribution trees.

If Multicast traffic is to be routed through a part of a network that does not support multicasting (routers which are not multicast capable) then the multicast packets are encapsulated in an IP datagram and sent as a unicast packet. When the multicast router at the remote end of the tunnel receives the packet, the router strips off the IP encapsulation and forwards the packet as an IP Multicast packet. This process of encapsulating multicast packets in IP is called tunneling.

To display the **IP Multicast** menu page, click **IP Multicast** in the tree view. The **IP Multicast** menu page contains links to the following features:

- Multicast
- Multicast Listener Discovery
- Distance Vector Multicast Routing Protocol
- Internet Group Management Protocol
- Protocol Independent Multicast-Dense Mode
- Protocol Independent Multicast-Sparse Mode

Downloaded from www.Manualslib.com manuals search engine

Multicast

The **Multicast** menu page contains links to web pages that define and display **Multicast** parameters and data. To display this page, click **IP Multicast** > **Multicast** in the tree view. Following are the web pages accessible from this menu page:

- Multicast Global Configuration
- Multicast Interface Configuration
- Multicast Mroute Summary
- Multicast Static Routes Configuration
- Multicast Static Routes Summary
- Multicast Admin Boundary Configuration
- Multicast Admin Boundary Summary

Multicast Global Configuration

Use the **Multicast Global Configuration** page to configure the administrative status of Multicast Forwarding in the router, and to display global multicast parameters.

To display the page, click **IP Multicast** > **Multicast** > **Global Configuration** in the tree view.

Figure 12-1. Multicast Global Configuration

Downloaded from www.Manualslib.com manuals search engine

The **Multicast Global Configuration** page contains the following fields:

- **Admin Mode** — Select Enable or Disable to set the administrative status of Multicast Forwarding in the router. The default is Disable.
- **Protocol State** — The operational state of the multicast forwarding module.
- **Table Maximum Entry Count** — The maximum number of entries in the IP Multicast routing table.
- **Number Of Packets For Which Source Not Found** — The number of multicast packets that were supposed to be routed but which failed the RPF check.
- **Number Of Packets For Which Group Not Found** — The number of multicast packets that were supposed to be routed but for which no multicast route was found.
- **Protocol** — The multicast routing protocol presently activated on the router, if any.
- **Table Entry Count** — The number of multicast route entries currently present in the Multicast route table.
- **Table Highest Entry Count** — The highest number of multicast route entries that have been present in the Multicast route table.

Downloaded from www.Manualslib.com manuals search engine

Configuring Multicast Forwarding Administrative Mode

1. Open the **Multicast Global Configuration** page.
2. Select Enable or Disable for the **Admin Mode**.
3. Click **Apply Changes**.

   The multicast global configuration is saved, and the device is updated.

Configuring/Displaying Multicast Forwarding Parameters using the CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide:*

- Multicast Commands

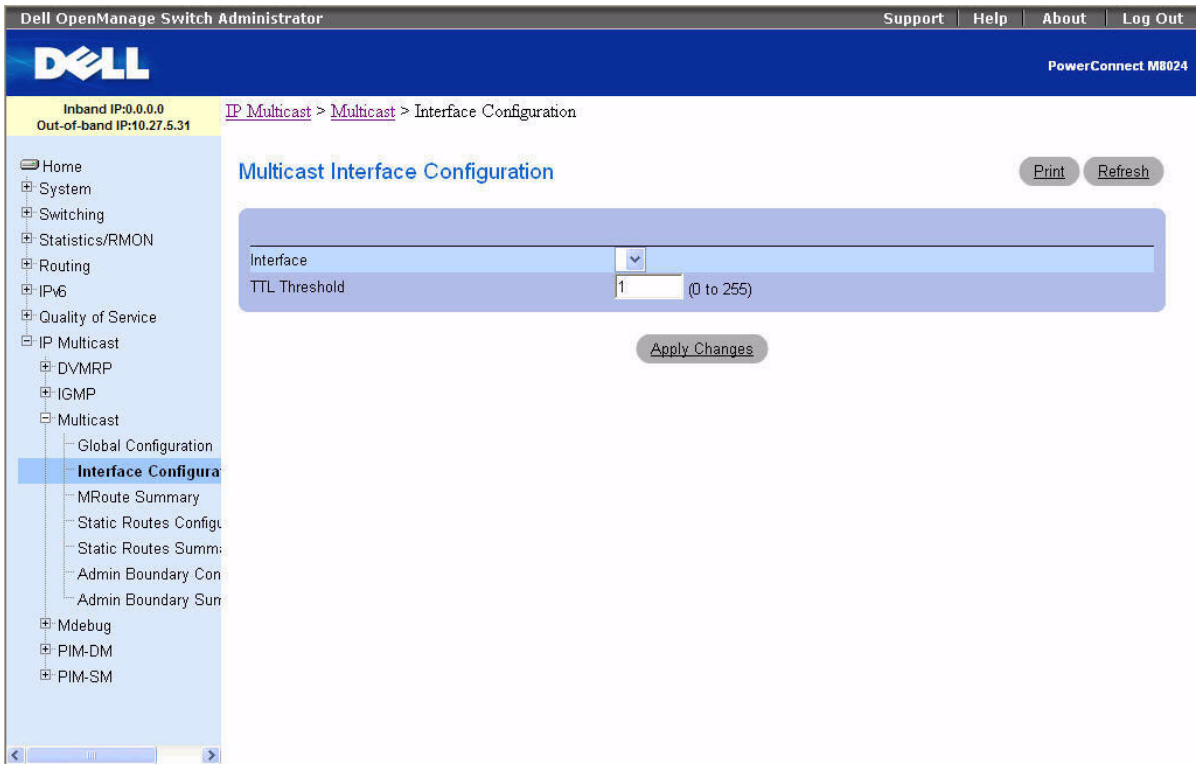
Downloaded from www.Manualslib.com manuals search engine

Multicast Interface Configuration

Use the **Multicast Interface Configuration** page to configure the TTL threshold of a multicast interface. You must configure at least one router interface before fields display on this page.

To display the page, click **IP Multicast > Multicast > Interface Configuration** in the tree view.

Figure 12-2. Multicast Interface Configuration



The **Multicast Interface Configuration** page contains the following fields:

- **Interface** — Select the routing interface you want to configure from the drop-down menu.
- **TTL Threshold** — Enter the TTL threshold below which a multicast data packet is not forwarded from the selected interface. Enter a number between 0 and 255. If you enter 0, all multicast packets for the selected interface are forwarded. You must configure at least one router interface to see this field.

Configuring a Multicast Interface

1. Open the **Multicast Interface Configuration** page.
2. Select the interface to configure from the **Interface** drop-down menu.
3. Enter the desired **TTL Threshold**.
4. Click **Apply Changes**.

   The multicast interface configuration is saved, and the device is updated.

Downloaded from www.Manualslib.com manuals search engine

Configuring a Multicast Interface using the CLI Command

For information about the CLI command that performs this function, see the following chapter in the *CLI Reference Guide:*

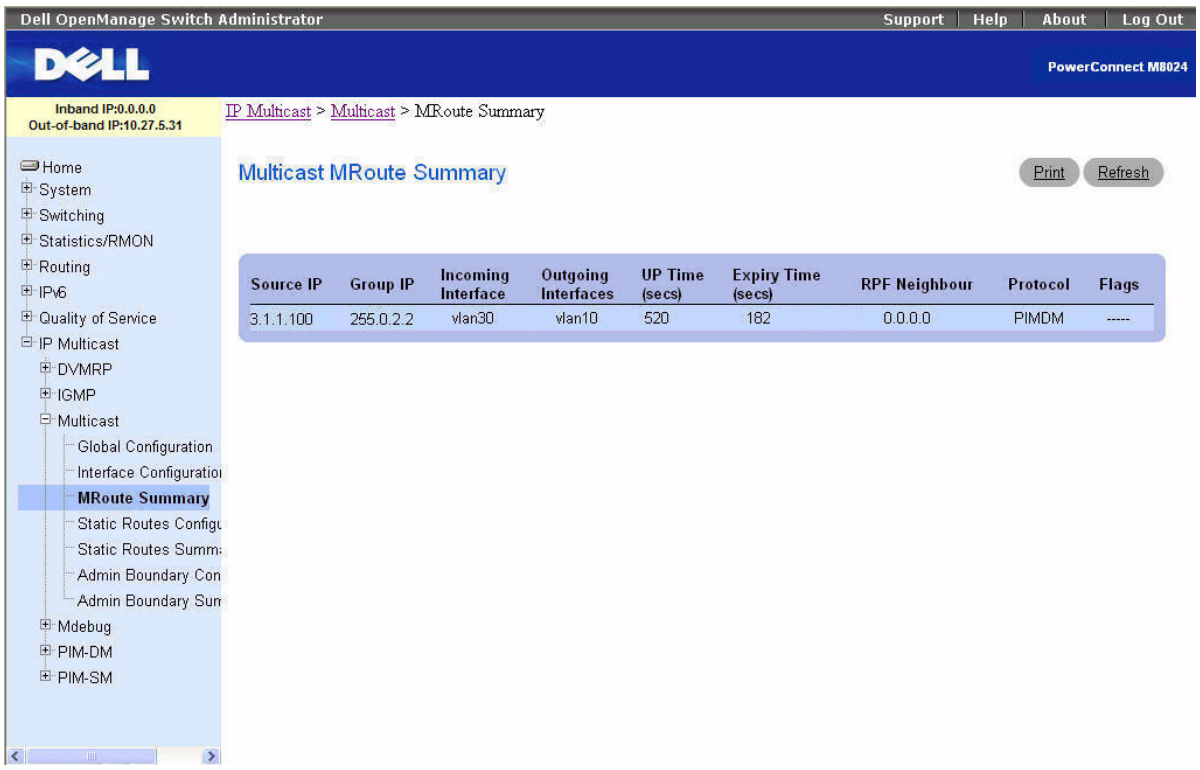
- Multicast Commands

Multicast Mroute Summary

Use the **Multicast Mroute Summary** page to display MRoute data.

To display the page, click **IP Multicast** > **Multicast** > **MRoute Summary** in the tree view.

Figure 12-3. Multicast Mroute Summary



The **Multicast Mroute Summary** page displays the following fields:

- **Source IP** — The IP address of the multicast packet source that, combined with the Group IP, identifies an Mroute table entry.
- **Group IP** — The destination group IP address.
- **Incoming Interface** — The incoming interface on which multicast packets for this source/group arrive.
- **Outgoing Interfaces** — The list of outgoing interfaces on which multicast packets for this source/group are forwarded.
- **Up Time (secs)** — The time in seconds since the entry was created.

Downloaded from www.Manualslib.com manuals search engine

- **Expiry Time (secs)** — The time in seconds before this entry ages out and is removed from the table.
- **RPF Neighbor** — The IP address of the Reverse Path Forwarding neighbor.
- **Protocol** — The multicast routing protocol which created this entry. The possibilities are:
  - **PIM-DM**
  - **PIM-SM**
  - **DVMRP**
- **Flags** — The value displayed in this field is valid if the multicast routing protocol running is PIM-SM. The possible values are RPT or SPT. For other protocols an "------" is displayed.

Displaying MRoute Summary using the CLI Command

For information about the CLI command that performs this function, see the following chapter in the *CLI Reference Guide:*

- Multicast Commands

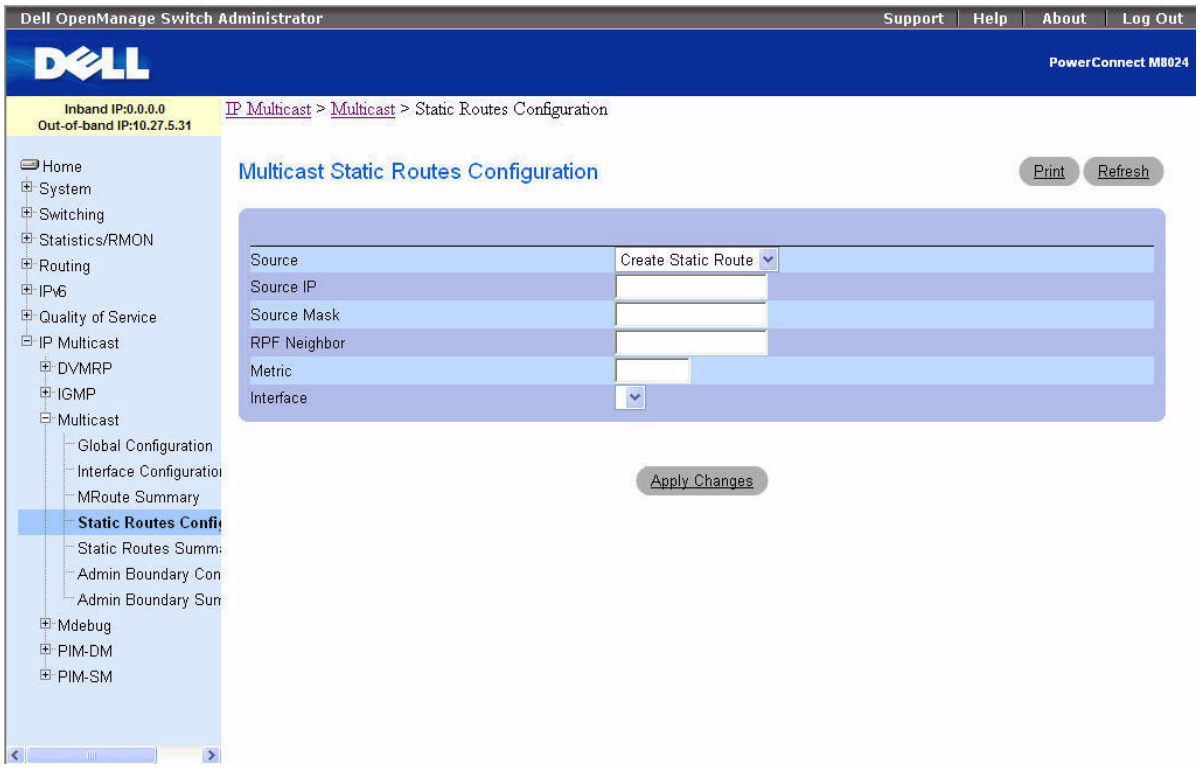
Downloaded from www.Manualslib.com manuals search engine

Multicast Static Routes Configuration

Use the **Multicast Static Routes Configuration** page to configure a new static entry in the Mroute table or to modify an existing entry.

To display the page, click **IP Multicast > Multicast > Static Routes Configuration** in the tree view.

Figure 12-4. Multicast Static Routes Configuration



The **Multicast Static Routes Configuration** page contains the following fields:

- **Source** — Select **Create Static Route** to configure a new static entry in the Mroute table, or select one of the existing entries from the drop-down menu.
- **Source IP** — Enter the IP Address that identifies the multicast packet source for the entry you are creating.
- **Source Mask** — Enter the subnet mask to be applied to the Source IP address.
- **RPF Neighbor** — Enter the IP address of the neighbor router on the path to the source.
- **Metric** — Enter the link state cost of the path to the multicast source. The range is 0–255, and the default is 1. You can change the metric for a configured route by selecting the static route and editing this field.
- **Interface** — Select the interface number from the drop-down menu. This is the interface that connects to the neighbor router for the given source IP address.

Downloaded from www.Manualslib.com manuals search engine

Configuring a Static Route

1. Open the **Static Routes** page.
2. Select **Create Static Route** in the **Source** field to configure a new static entry, or select one of the existing entries.
3. Modify the remaining fields as needed.
4. Click **Apply Changes**.

   The new or modified static route is saved, and the device is updated.

Configuring a Static Route the CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide:*

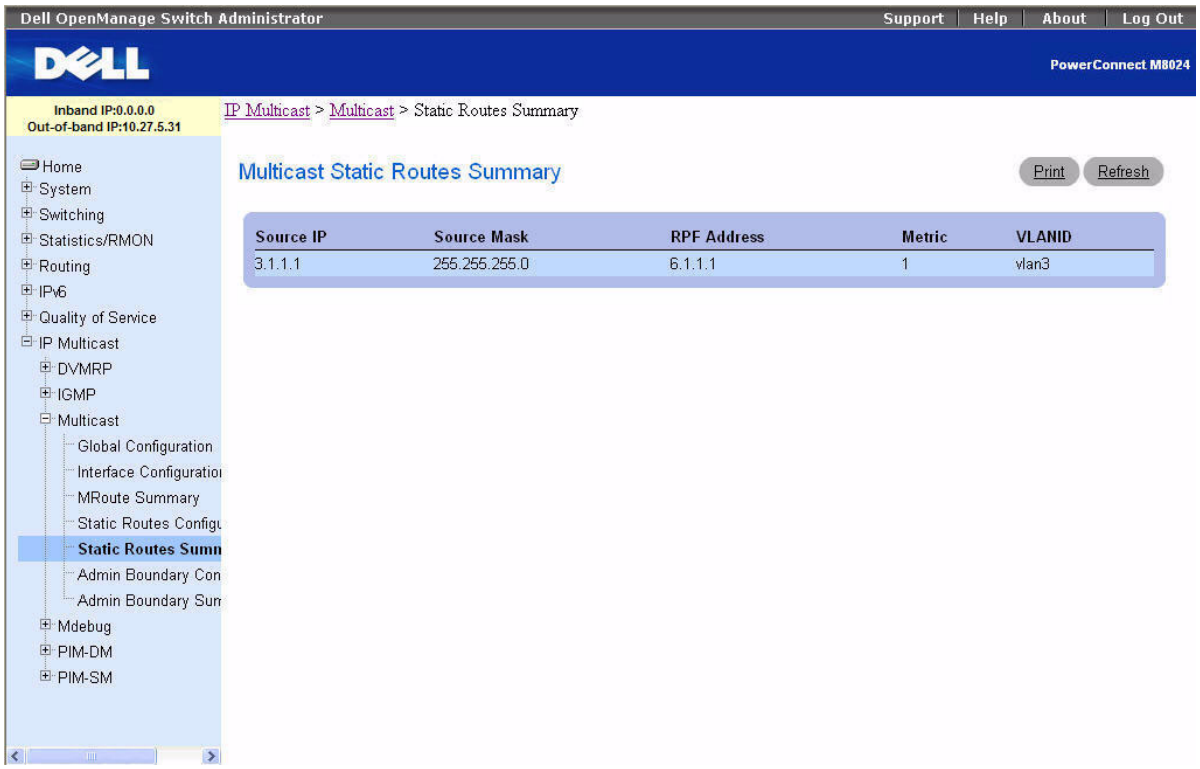
- Multicast Commands

Multicast Static Routes Summary

Use the **Multicast Static Routes Summary** page to display static routes and their configurations.

To display the page, click **IP Multicast > Multicast > Static Routes Summary** in the tree view.

Figure 12-5. Multicast Static Routes Summary



Downloaded from www.Manualslib.com manuals search engine

The **Multicast Static Routes Summary** page displays the following fields:

- **Source IP** — The IP Address that identifies the multicast packet source for this route.
- **Source Mask** — The subnet mask applied to the Source IP address.
- **RPF Address** — The IP address of the RPF neighbor.
- **Metric** — The link state cost of the path to the multicast source. The range is 0–255.
- **VLANID** — The number of the incoming VLAN whose IP address is used as RPF for the given source IP address.

Displaying the Static Routes Summary using the CLI Command

For information about the CLI command that performs this function, see the following chapter in the *CLI Reference Guide:*

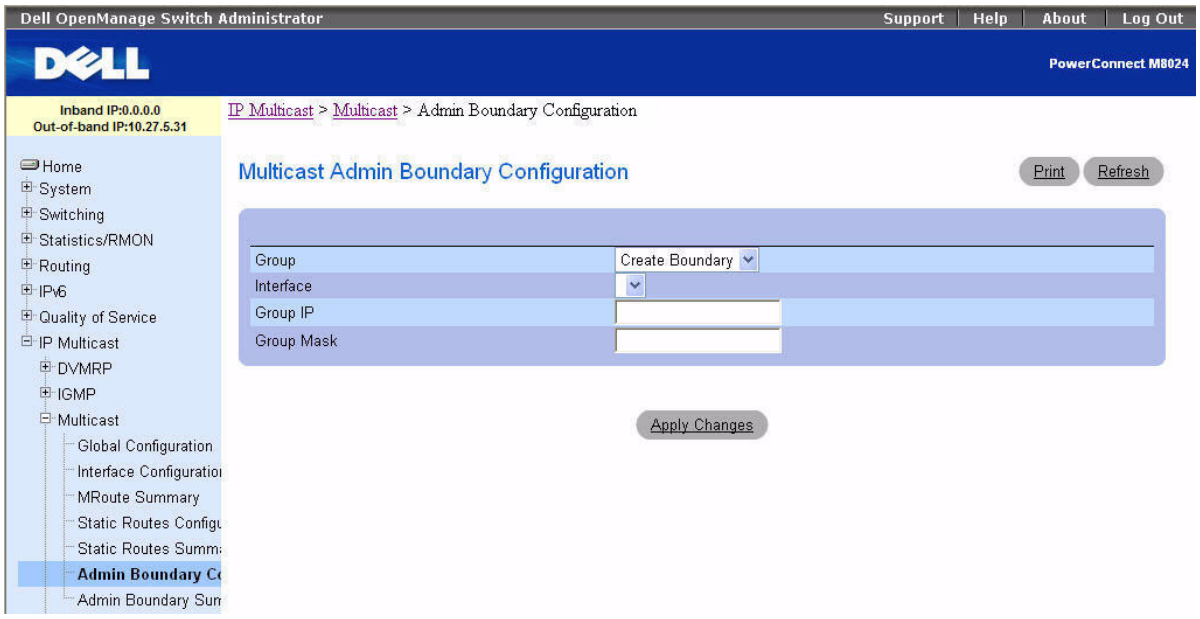
- Multicast Commands

Multicast Admin Boundary Configuration

The definition of an administratively scoped boundary is a way to stop the ingress and egress of multicast traffic for a given range of multicast addresses on a given routing interface. Use the **Multicast Admin Boundary Configuration** page to configure a new or existing administratively scoped boundary. To see this page, you must have configured a valid routing interface and multicast.

To display the page, click **IP Multicast > Multicast > Admin Boundary Configuration** in the tree view.

Figure 12-6. Multicast Admin Boundary Configuration



Downloaded from www.Manualslib.com manuals search engine

The **Multicast Admin Boundary Configuration** page contains the following fields:

- **Group** — Select **Create Boundary** from the drop-down menu to create a new admin scope boundary, or select one of the existing boundary specifications to display or update its configuration.
- **Interface** — Select the router interface for which the administratively scoped boundary is to be configured.
- **Group IP** — Enter the multicast group address for the start of the range of addresses to be excluded. The address must be in the range of 239.0.0.0 through 239.255.255.255.
- **Group Mask** — Enter the mask to be applied to the multicast group address. The combination of the mask and the Group IP gives the range of administratively scoped addresses for the selected interface.

Configuring an Admin Boundary

1. Open the **Multicast Admin Boundary Configuration** page.
2. Select **Create Boundary** in the **Group IP** field to configure a new admin scope boundary, or select one of the existing entries.
3. Modify the remaining fields as needed.
4. Click **Apply Changes**.

   The new or modified admin scope boundary is saved, and the device is updated.

Configuring an Admin Boundary using the CLI Command

For information about the CLI command that performs this function, see the following chapter in the *CLI Reference Guide:*

- Multicast Commands

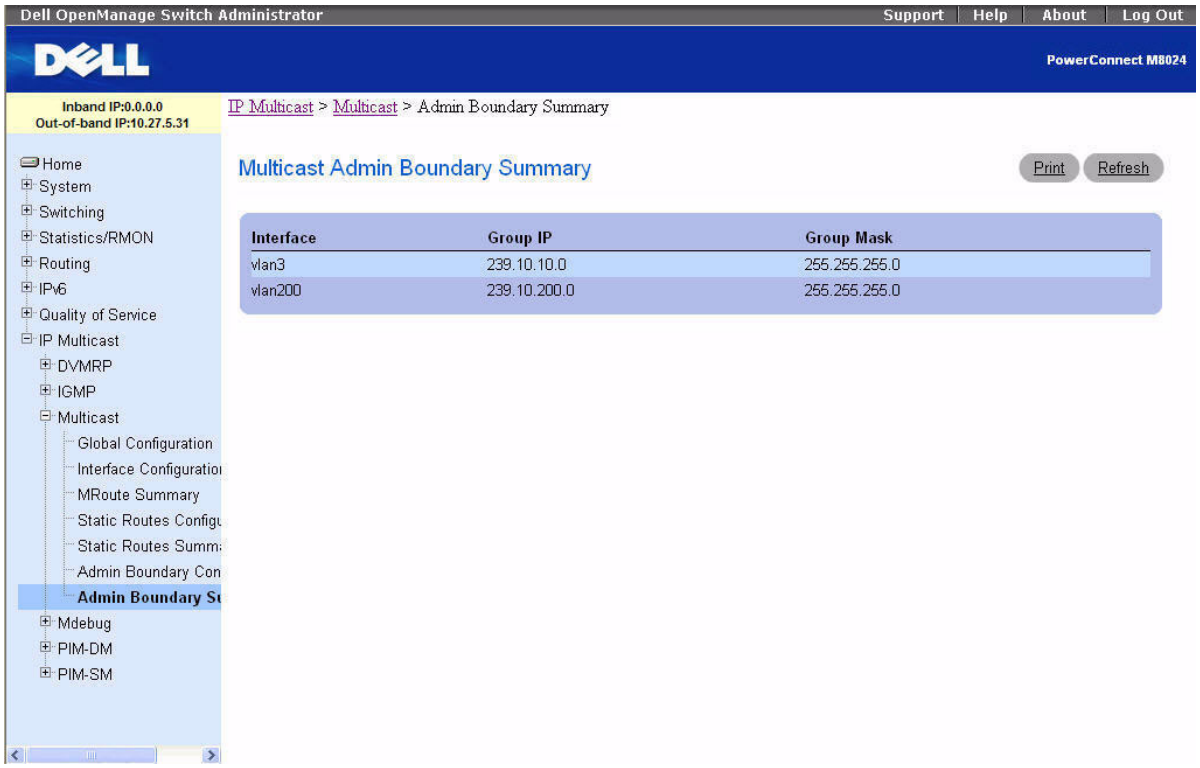
Downloaded from www.Manualslib.com manuals search engine

Multicast Admin Boundary Summary

Use the **Multicast Admin Boundary Summary** page to display existing administratively scoped boundaries.

To display the page, click **IP Multicast > Multicast > Admin Boundary Summary** in the tree view.

Figure 12-7. Multicast Admin Boundary Summary



The **Multicast Admin Boundary Summary** page displays the following fields:

- **Interface** — The router interface to which the administratively scoped address range is applied.
- **Group IP** — The multicast group address for the start of the range of addresses to be excluded.
- **Group Mask** — The mask that is applied to the multicast group address. The combination of the mask and the Group IP gives the range of administratively scoped addresses for the selected interface.

Displaying the Multicast Admin Boundary Summary using the CLI Command

For information about the CLI command that performs this function, see the following chapter in the *CLI Reference Guide:*

- Multicast Commands

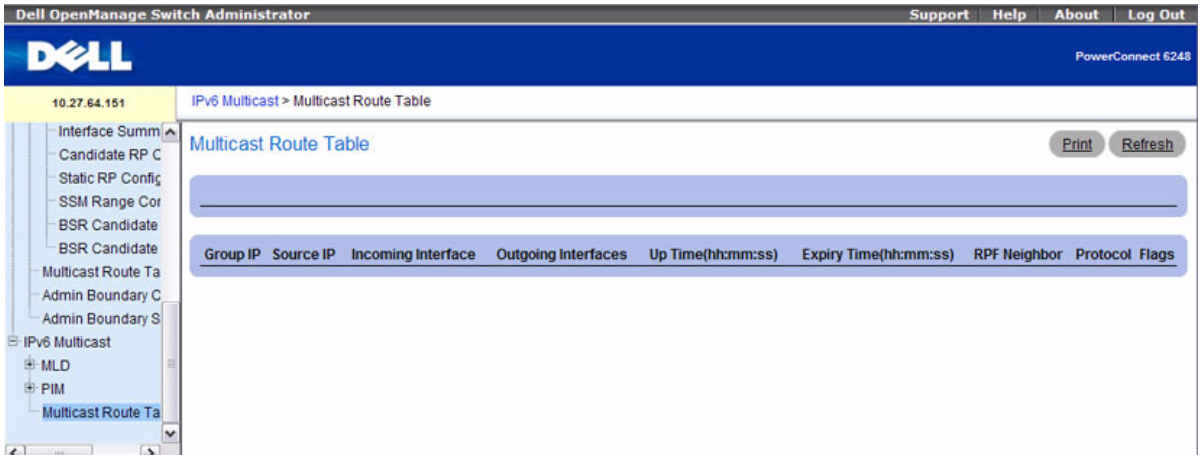
Downloaded from www.Manualslib.com manuals search engine

Multicast Route Table

Use the **Multicast Route Table** page is used to display MRoute data.

To display the page, click **IPv4 Multicast > Multicast > Multicast Route Table** or **IPv6 Multicast > Multicast > Multicast Route Table**.

Figure 12-8. Multicast Route Table



The **Multicast Route Table** page contains the following fields:

- **Group IP** — The destination group IP address.
- **Source IP** — The IP address of the multicast packet source that, combined with the Group IP, identifies an multicast route table entry.
- **Incoming Interface** — The incoming interface on which multicast packets for this source/group arrive.
- **Outgoing Interfaces** — The list of outgoing interfaces on which multicast packets for this source/group are forwarded.
- **Up Time** — The time in hours:minutes:seconds since the entry was created.
- **Expiry Time** — The time in hours:minutes:seconds before this entry ages out and is removed from the table.
- **RPF Neighbor** — The IP address of the Reverse Path Forwarding neighbor.
- **ProtocolFlags** — The multicast routing protocol which created this entry. The possibilities are:
  - **PIM-DM**
  - **PIM-SM**
  - **DVMRP**
- **Flags** — The value displayed in this field is valid if the multicast routing protocol running is PIM-SM. The possible values are RPT or SPT. For other protocols a "------" (no value) is displayed.

Downloaded from www.Manualslib.com manuals search engine

Multicast Listener Discovery

Multicast Listener Discovery (MLD) protocol enables IPv6 routers to discover the presence of multicast listeners, the nodes who wish to receive the multicast data packets, on its directly-attached interfaces. The protocol specifically discovers which multicast addresses are of interest to its neighboring nodes and provides this information to the active multicast routing protocol that makes decisions on the flow of multicast data packets.

The Multicast router sends General Queries periodically to request multicast address listeners information from systems on an attached network. These queries are used to build and refresh the multicast address listener state on attached networks. Multicast listeners respond to these queries by reporting their multicast addresses listener state and their desired set of sources with Current-State Multicast address Records in the MLD2 Membership Reports. The Multicast router also processes unsolicited Filter-Mode-Change records and Source-List-Change Records from systems that want to indicate interest in receiving or not receiving traffic from particular sources.

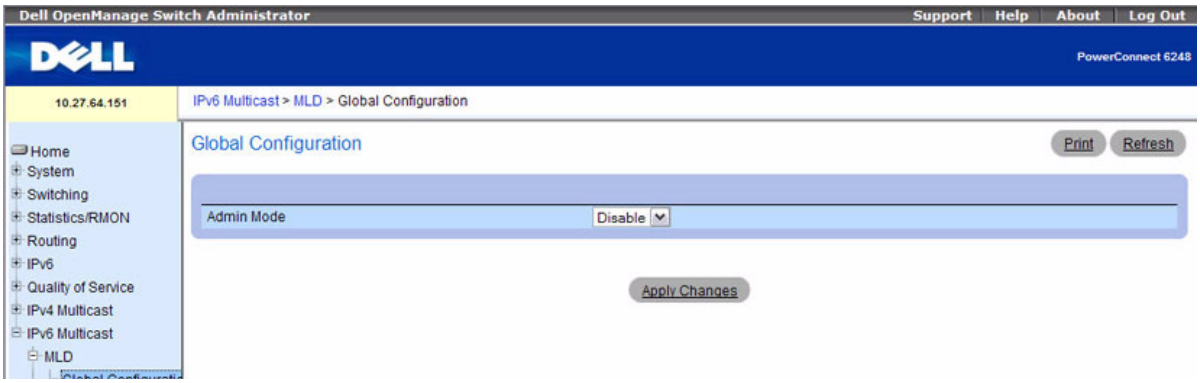
The FASTPATH implementation of MLD v2 supports the multicast router portion of the protocol (i.e., not the listener portion). It is backward-compatible with MLD v1.

MLD Global Configuration

Use the **MLD Global Configuration** page to administratively enable and disable the MLD service.

To display the page, click **IPv6 Multicast > MLD > Global Configuration** in the tree view.

Figure 12-9. MLD Global Configuration



Downloaded from www.Manualslib.com manuals search engine

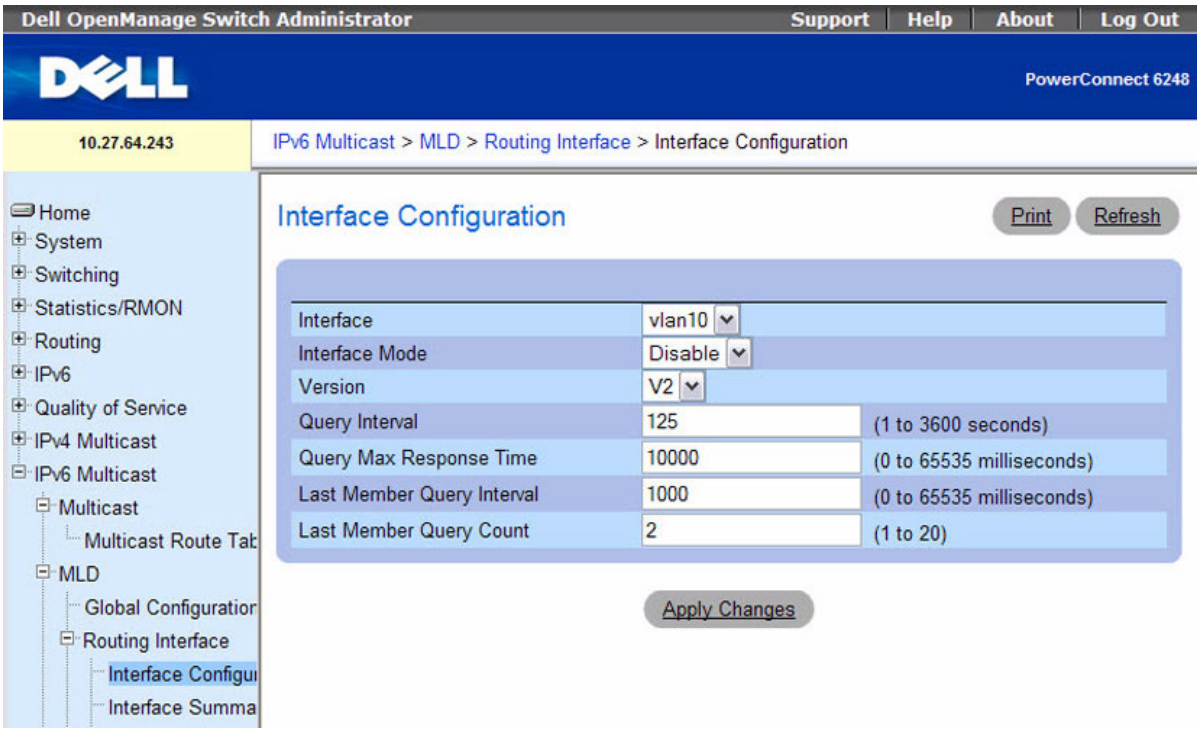
The **MLD Global Configuration** page contains the following field:

- **Admin Mode** — Select Enable or Disable to set the MLD administrative status. The default is disable. Click **Apply Changes** to send the updated configuration to the router. Configuration changes take effect immediately. These changes will not be retained across a power cycle unless a save is performed.

MLD Routing Interface Configuration

Use the **MLD Routing Interface Configuration** page to enable selected IPv6 router interfaces to discover the presence of multicast listeners, the nodes who wish to receive the multicast data packets, on its directly attached interfaces. To access this page, click **IPv6 Multicast > MLD > Routing Interface > Interface Configuration** in the navigation tree.

Figure 12-10. MLD Routing Interface Configuration



The **MLD Routing Interface Configuration** page contains the following fields:

- **Interface** — From the drop-down menu, select the VLAN routing interface to be configuration.
- **Interface Mode** — Select **Enable** or **Disable** to set the administrative status of MLD on the selected interface. The default is **Disable**.
- **Version** — Select the MLD version.
- **Query Interval** — Specify the number of seconds between MLD general queries. Valid values are 1 to 3600. The default value is 125.

Downloaded from www.Manualslib.com manuals search engine

- **Query Max Response Time (secs)** — Enter the maximum query response time to be advertised in MLDv2 queries on this interface, in ms. The default value is 10000. Valid values are 0 to 65535 milliseconds (ms).
- **Last Member Query Interval** — Enter the maximum response time inserted into group-specific queries sent in response to leave group messages. This value is also the amount of time between group-specific query messages. This value may be tuned to modify the leave latency of the network. Valid values are 0 to 65535 milliseconds (ms). The default is 1000.
- **Last Member Query Count** — The number of queries to be sent on receiving a leave group report. Valid values are 1 to 20. The default is 2.

MLD Routing Interface Summary

Use the **MLD Routing Interface Summary** page to display information and statistics on a selected MLD-enabled interface. You must configure at least one IGMP router interface to access this page.

To access this page, click **IPv6 Multicast > MLD > Routing Interface > Interface Summary** in the navigation tree.

Figure 12-11. MLD Routing Interface Summary

Downloaded from www.Manualslib.com manuals search engine

The **MLD Routing Interface Summary** page contains the following fields:

- **Interface** — Select the VLAN for which data is to be displayed.

Interface Parameters section:

- **Global Admin Mode** — Displays whether MLD has been globally enabled or disabled.
- **Interface Mode** — Displays whether the administrative status of MLD on the selected interface is enabled or disabled.
- **Operational Mode** — Displays the operational state of MLD on the selected interface, regardless of the administrative setting.
- **Version** — Displays the version of MLD configured on the selected interface.
- **Query Interval** — Displays the interval in seconds at which MLD host-query packets are transmitted on the selected interface.
- **Query Max Response Time** — Displays the maximum query response time in milliseconds (ms) advertised in MLDv2 queries from the selected interface.
- **Robustness** — Displays the robustness parameter for the selected interface. This value allows tuning for the expected packet loss on a subnet. If a subnet is expected to be lossy, increase the robustness variable. MLD is robust to (robustness variable - 1) packet losses.
- **Startup Query Interval** — Displays the interval in seconds at which startup queries are sent on the selected interface.
- **Startup Query Count** — Displays the number of queries to be sent upon startup.
- **Last Member Query Interval** — Displays the maximum response time, in milliseconds, inserted into group-specific queries sent in response to leave group messages. This value is also the amount of time between group-specific query messages. This value may be tuned to modify the leave latency of the network. This value may be tuned to modify the leave latency of the network. A reduced value results in reduced time to detect the loss of the last member of a group.

NOTE: This value is not used for MLD version 1.

- **Last Member Query Count** — The number of queries to be sent on receiving a leave group report.

Interface Statistics section:

- **Querier Status** — Displays whether the selected router interface is currently the MLD querier. If another interface on the network has a lower source IP address, it becomes the querier.
- **Querier** — The address of the MLD querier on the IP subnet to which the selected interface is attached.
- **Querier Up Time** — The time in hours:minutes:seconds since the MLD interface querier was last changed.
- **Querier Expiry Time** — The time in hours:minutes:seconds remaining before the other querier present timer expires. If the local system is the querier, this will be zero.

Downloaded from www.Manualslib.com manuals search engine

- **Wrong Version Queries Received** — The number of queries that have been received on the selected interface with an MLD version that does not match the MLD version configured for the interface, over the lifetime of the entry. MLD requires that all routers on a LAN be configured to run the same version of MLD. Therefore, a configuration error is indicated if any queries are received with the wrong version number.
- **Number of Joins Received** — The number of times a group membership has been added on the selected interface; that is, the number of times an entry for this interface has been added to the cache table. This gives an indication of the amount of MLD activity on the interface.
- **Number of Groups** — The current number of entries for the selected interface in the cache table.

Click **Refresh** to display the latest information from the router.

MLD Routing Interface Cache Information

The **MLD Routing Interface Cache Information** page displays cache parameters and data for an IP multicast group address that has been reported to operational MLD routing interfaces. You must configure at least one MLD router interface to access this page. Also, group membership reports must have been received on the selected interface in order for data to be displayed here. To access this page, click **IPv6 Multicast > MLD > Routing Interface > Cache Information** in the navigation tree.

Figure 12-12. MLD Routing Interface Cache Information

The **MLD Routing Interface Cache Information** page contains the following fields:

- **Multicast Group IP** — Select the IP multicast group address for which data is to be displayed. Only if group membership reports have been received on the selected interface can you make this selection, and the data on this page displays.
- **Interface** — Select the MLD routing interface for which data is displayed.

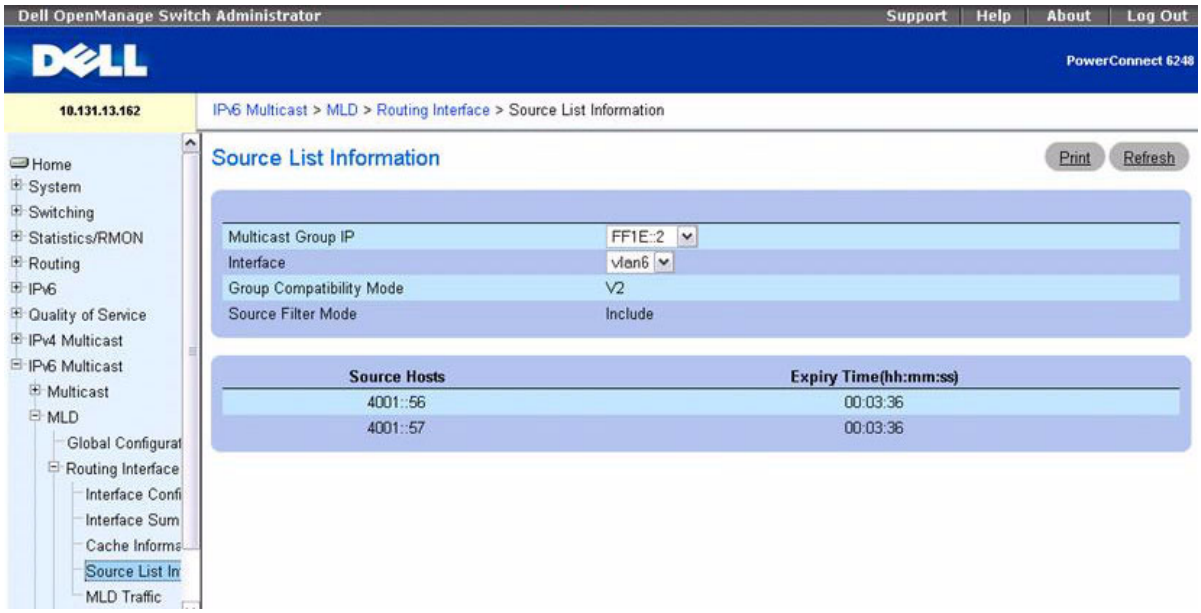
Downloaded from www.Manualslib.com manuals search engine

- **Last Reporter** — The IP Address of the source of the last membership report received for this IP Multicast group address on the selected interface.
- **Up Time** — The time elapsed in hours:minutes:seconds since this entry was created.
- **Expiry Time** — The cache timer value which indicates the remaining lifetime in hours:minutes:seconds for each entry.
- **Version1 Host Timer** — The time in hours:minutes:seconds remaining until the local router assumes that there are no longer any MLD version 1 members on the IP subnet attached to this interface. When an MLDv1 membership report is received, this timer is reset to the group membership timer.
- **Compatibility** — The compatibility mode (V1, V2) for this multicast group on the specified interface.
- **Filter Mode** — The source filter mode for the specified multicast group on this interface. Possible values are **Include, Exclude** and **NA**. When **NA** mode is active, this field is blank.

MLD Routing Interface Source List Information

The **MLD Routing Interface Source List Information** page displays detailed membership information for an interface. You must configure at least one MLD router interface to access this page. Also, group membership reports must have been received on the selected interface in order for data to be displayed here. To access this page, click **IPv6 Multicast > MLD > Routing Interface > Source List Information** in the navigation tree.

Figure 12-13. MLD Routing Interface Source List Information



Downloaded from www.Manualslib.com manuals search engine

The **MLD Routing Interface Source List Information** page contains the following fields:

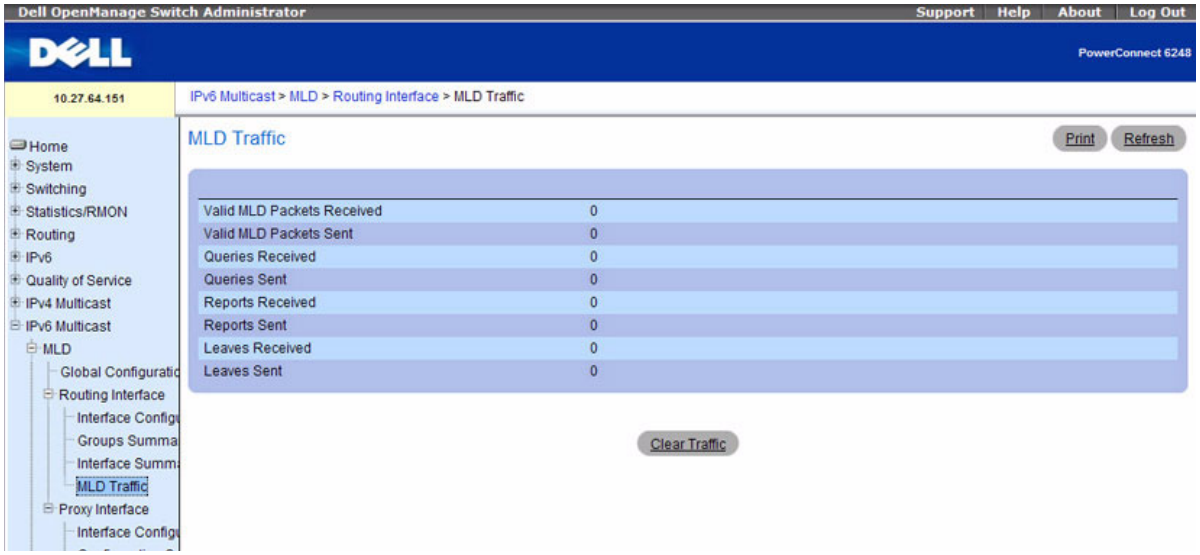
- **Multicast Group IP** — Select the IP multicast group address for which data is to be displayed. Only if group membership reports have been received on the selected interface can you make this selection, and the data on this page displays.
- **Interface** — Select the MLD routing interface for which data is displayed.
- **Group Compatibility Mode** — The compatibility mode (V1, V2) for this multicast group on the specified interface.
- **Source Filter Mode** — The source filter mode for the specified multicast group on this interface. Possible values are **Include, Exclude** and **NA**. When **NA** mode is active, this field is blank.
- **Source Hosts** — The source addresses which are members of this multicast address.
- **Expiry Time** — The expiry time interval in hours:minutes:seconds for each source address that is a member of this multicast group. This is the length of time after which the specified source entry is aged. out.

MLD Traffic

The **MLD Traffic** page displays summary statistics on the MLD messages sent to and from the router.

To access this page, click **IPv6 Multicast > MLD > Routing Interface > MLD Traffic** in the navigation tree.

Figure 12-14. MLD Traffic



Downloaded from www.Manualslib.com manuals search engine

The **MLD Traffic** page contains the following fields:

- **Valid MLD Packets Received** — The total number of valid MLD packets received by the router.
- **Valid MLD Packets Sent** — The total number of valid MLD packets sent from the router
- **Querier Received** — The total number of MLD packets sent as the MLD querier.
- **Querier Sent** — The total number of MLD packets sent as the MLD querier.
- **Reports Received** — The total number of MLD reports received.
- **Reports Sent** — The total number of MLD reports received.
- **Leaves Received** — The total number of MLD Leave messages received.
- **Leaves Sent** — The total number of MLD Leave messages received.

Click **Refresh** to display the latest information from the router.

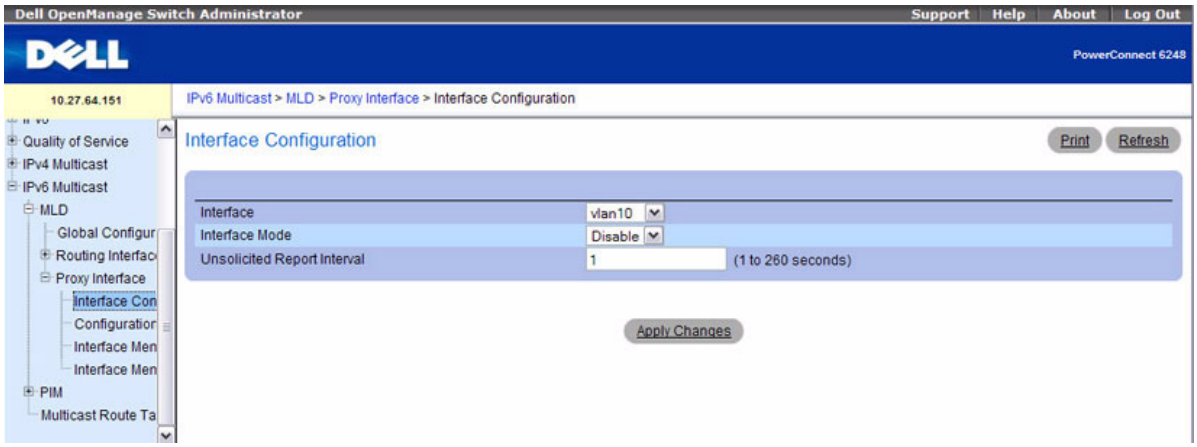
Click **Clear Traffic** to reset all counters to their default values.

MLD Proxy Configuration

When you configure an interface in MLD proxy mode, it acts as a proxy multicast host that sends MLD membership reports on one interface for MLD Membership reports received on all other MLD-enabled router interfaces.

Use the **MLD Proxy Interface Configuration** page to enable and disable ports as MLD proxy interfaces. To display this page, click **IPv6 Multicast > MLD > Proxy Interface > Interface Configuration** in the navigation tree.

Figure 12-15. MLD Proxy Interface Configuration



Downloaded from www.Manualslib.com manuals search engine

The **MLD Proxy Interface Configuration** page contains the following fields:

- **Interface** — Select the interface for which data is to be displayed or configured from the menu. You must have configured at least one router interface before configuring or displaying data for an MLD Proxy interface and it should not be a MLD routing interface.
- **Interface Mode** — Select enable or disable from the menu to set the administrative status of MLD Proxy on the selected interface. The default is disable. Routing, MLD and Multicast global admin modes should be enabled to enable MLD Proxy interface mode.
- **Unsolicited Report Interval** — Enter the unsolicited time interval value in seconds. The Unsolicited Report Interval is the time between repetitions of a host's initial report of membership in a group. Valid values are from (1 to 260). The default value is 1.

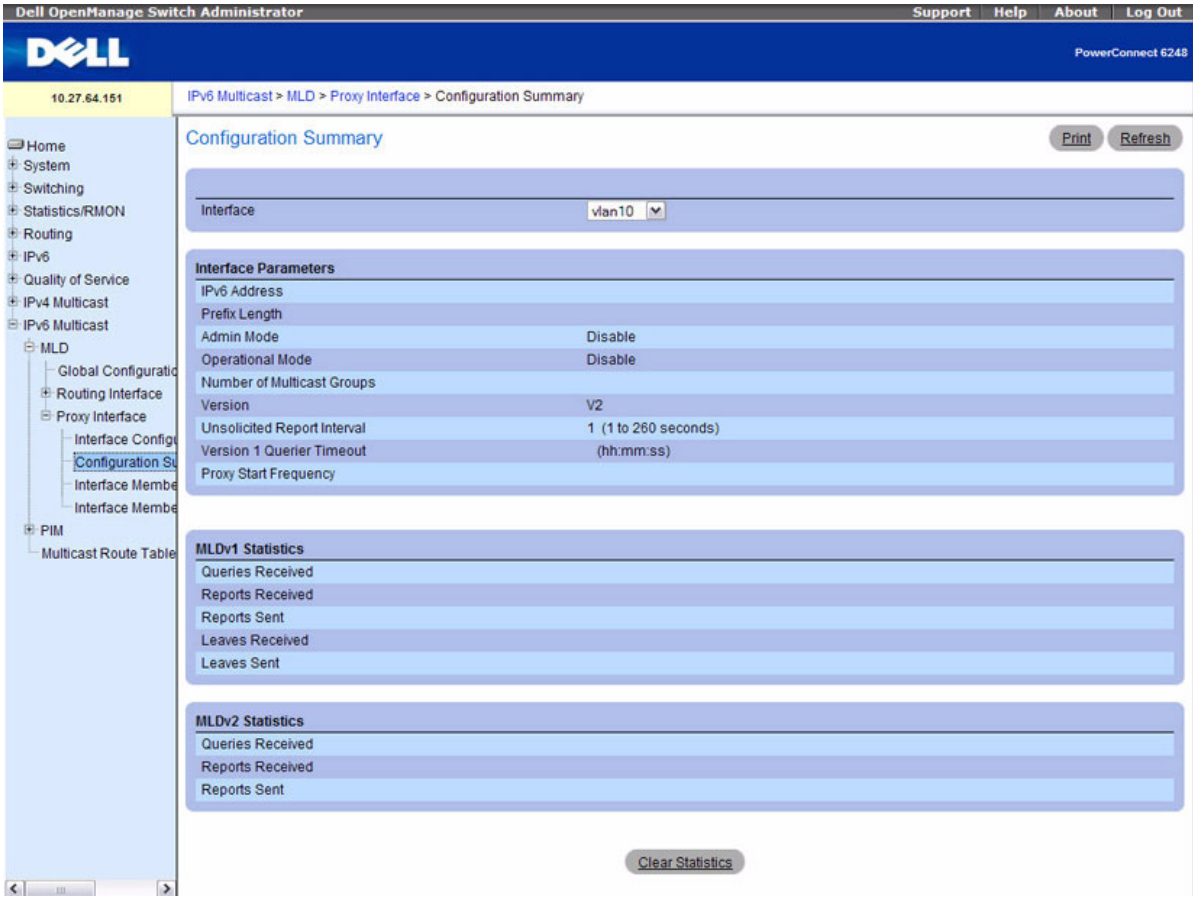
Click **Apply Changes** to send the updated configuration to the switch. Configuration changes take effect immediately. These changes will not be retained across a power cycle unless a save is performed.

Downloaded from www.Manualslib.com manuals search engine

MLD Proxy Configuration Summary

Use the **MLD Proxy Configuration Summary** page to view configuration and statistics on MLD proxy-enabled interfaces. To display this page, click **IPv6 Multicast > MLD > Proxy Interface > Configuration Summary** in the navigation tree.

Figure 12-16. MLD Proxy Configuration Summary



The **MLD Proxy Configuration Summary** page contains the following fields:

- **Interface** — Select the interface on which MLD proxy is enabled and for which data is to be displayed.
- **IPv6 Address** — The IPv6 address of the MLD Proxy interface.
- **Prefix Length** — Displays the prefix length for the IPv6 address of the MLD Proxy interface.
- **Admin Mode** — The administrative status of MLD Proxy on the selected interface.
- **Operational Mode** — The operational state of MLD Proxy interface.
- **Number of Multicast Groups** — The current number of multicast group entries for the MLD Proxy interface in the cache table.

Downloaded from www.Manualslib.com manuals search engine

- **Version** — The version of MLD configured on the MLD Proxy interface.
- **Unsolicited Report Interval** — The Unsolicited Report Interval in seconds is the time between repetitions of a host's initial report of membership in a group.
- **Version 1 Querier Timeout** — The older MLD version 1 querier timeout value in hours:minutes:seconds. The Older Version Querier Interval is the time-out for transitioning a host back to MLD mode once an older version query is heard. When an older version query is received, hosts set their Older Version Querier Present Timer to Older Version Querier Interval.
- **Proxy Start Frequency** — The number of times the proxy was brought up.

Click **Refresh** to refresh the data on the screen with the present state of the data in the router.

Click **Clear Statistics** to clear the MLD Proxy Interface statistics and reset the counters to their original values.

Interface Membership Information

The **Interface Membership Information** page lists each IP multicast group for which the MLD proxy interface has received membership reports. To display this page, click **IPv6 Multicast > MLD > Proxy interface > Interface Membership Info** in the navigation tree.

Figure 12-17. Interface Membership Information

Downloaded from www.Manualslib.com manuals search engine

The **Interface Membership Information** page contains the following fields:

- **Interface** — Displays the interface on which MLD proxy is enabled.
- **Multicast Group IP** — Select the IP multicast group address for which data is to be displayed. If no group membership reports have been received on the selected interface you will not be able to make this selection, and none of the non-configurable data will be displayed.
- **Last Reporter** — The IP address of the source of the last membership report received for the IP Multicast group address on the MLD Proxy interface.
- **Uptime** — The time elapsed since this entry was created. Displayed in hours:minutes:seconds.
- **State** — The state of the host entry. A host can be in one of the following states:
  - **Non-member**. Does not belong to the group on the interface.
  - **Delaying Member**. Host belongs to the group on the interface and report timer is running. The report timer is used to send out the reports.
  - **Idle Member**. Host belongs to the group on the interface and no report timer is running.
- **Filter Mode** — The group filter mode for the specified group on the MLD Proxy interface. Possible values are **Include**, **Exclude**, or **None**.
- **Number of Sources** — The number of source hosts present in the selected multicast group.

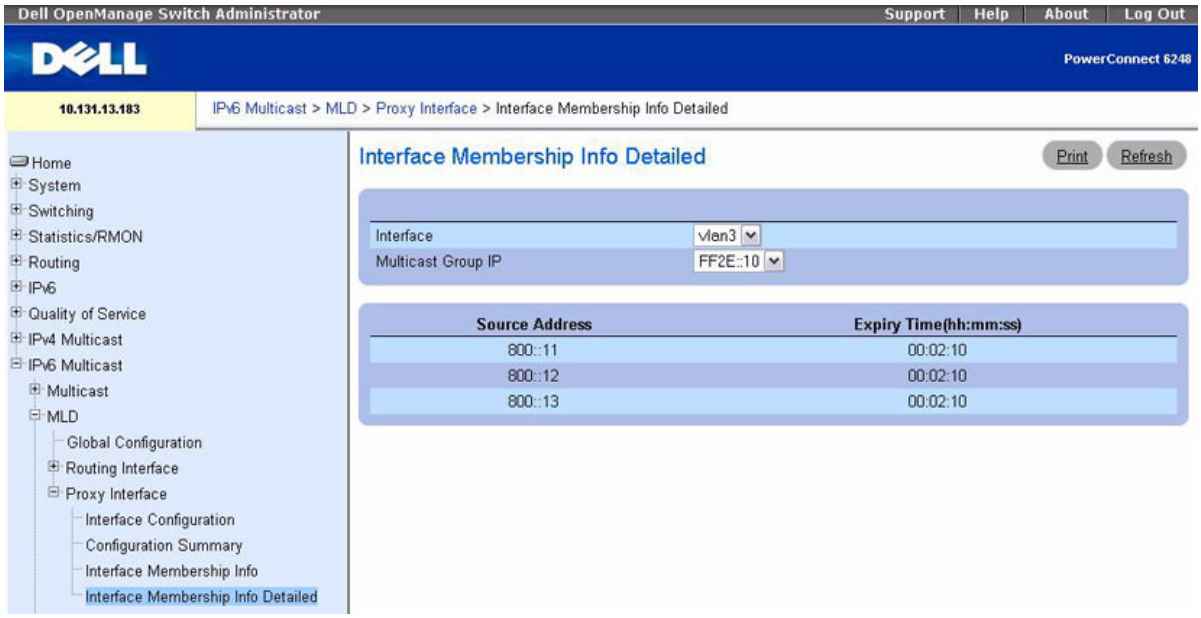
Click **Refresh** to refresh the data on the screen with the present state of the data in the router.

Downloaded from www.Manualslib.com manuals search engine

Interface Membership Information—Detailed

The **Interface Membership Information—Detailed** page provides additional information on the IP multicast groups for which the MLD proxy interface has received membership reports. To display this page, click **IPv6 Multicast > MLD > Proxy Interface > Interface Membership Info Detailed** in the navigation tree.

Figure 12-18. Interface Membership Information—Detailed



The **Interface Membership Information — Detailed** page contains the following fields:

- **Interface** — Select the interface on which MLD proxy is enabled for which data is to be displayed.
- **Multicast Group IP** — Select the IP multicast group address for which data is to be displayed. If no group membership reports have been received on the selected MLD Proxy interface you will not be able to make this selection, and none of the non-configurable data will be displayed.
- **Source Address** — This parameter shows source addresses which are members of this multicast address.
- **Expiry Time** — Displays the expiry time in hours:minutes:seconds since the entry was created in the cache table.

Click **Refresh** to refresh the data on the screen with the present state of the data in the router.

Downloaded from www.Manualslib.com manuals search engine

Distance Vector Multicast Routing Protocol

Distance Vector Multicast Routing Protocol (DVMRP) exchanges probe packets with all its DVMRP enabled routers, it establishes two way neighboring relationships, and it builds a neighbor table. It exchanges report packets and creates a unicast topology table, with which it builds the multicast routing table. This table is used to route the multicast packets. Since every DVMRP router uses the same unicast routing protocol, routing loops are avoided.

The **DVMRP** menu page contains links to web pages that define and display DVMRP parameters and data. To display this page, click **IP Multicast > DVMRP** in the tree view.

The following web pages are accessible from this menu page:

- DVMRP Global Configuration
- DVMRP Interface Configuration
- DVMRP Configuration Summary
- Next Hop Summary
- Prune Summary
- Route Summary

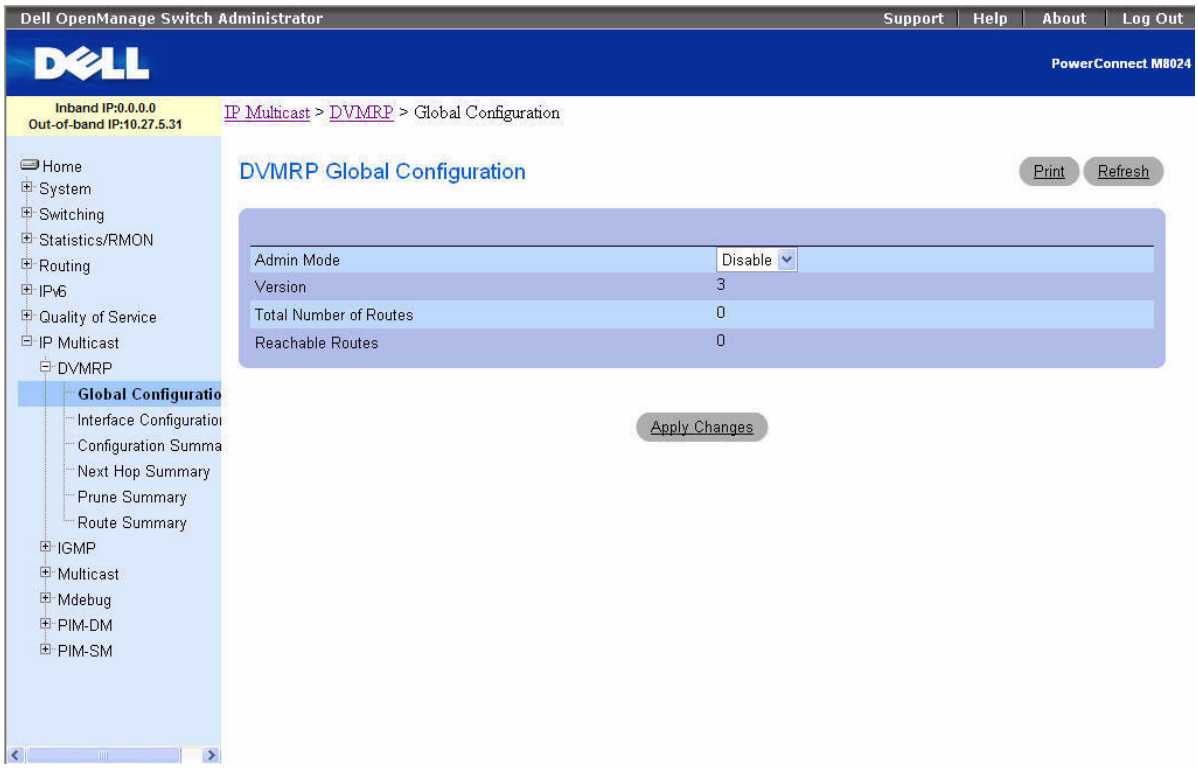
Downloaded from www.Manualslib.com manuals search engine

DVMRP Global Configuration

Use the **DVMRP Global Configuration** page to configure global DVMRP settings.

To display the page, click **IP Multicast > DVMRP > Global Configuration** in the tree view.

Figure 12-19. DVMRP Global Configuration



The **DVMRP Global Configuration** page contains the following fields:

- **Admin Mode** — Select Enable or Disable from the drop-down menu. This sets the administrative status of DVMRP to active or inactive. The default is Disable.
- **Version** — The current value of the DVMRP version string.
- **Total Number of Routes** — The number of routes in the DVMRP routing table.
- **Reachable Routes** — The number of routes in the DVMRP routing table that have a non-infinite metric.

Setting the DVMRP Admin Mode

1. Open the **DVMRP Global Configuration** page.
2. Set **Admin Mode** to Enable or Disable, to turn DVMRP on or off.
3. Click **Apply Changes**.

   The DVMRP configuration is saved, and the device is updated.

Downloaded from www.Manualslib.com manuals search engine

Configuring DVMRP using the CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide:*

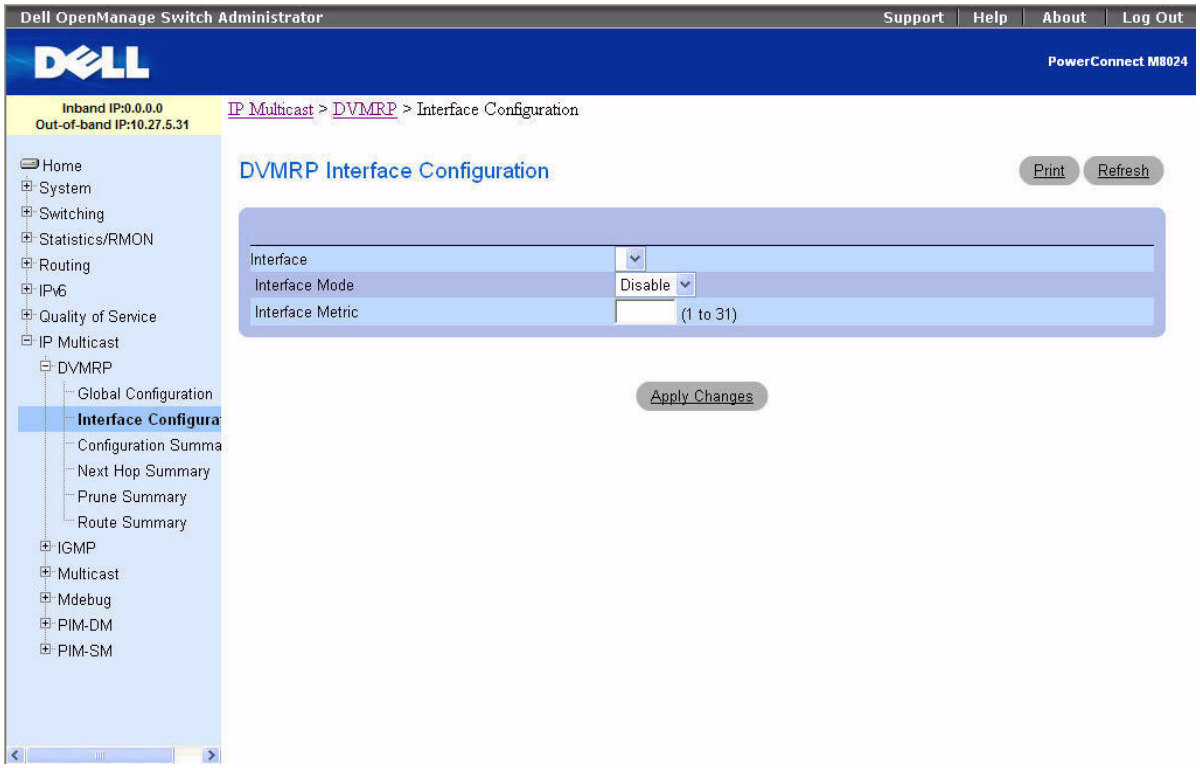
- DVMRP Commands

DVMRP Interface Configuration

Use the **DVMRP Interface Configuration** page to configure a DVMRP interface. You must configure at least one router interface before you configure a DVMRP interface. Otherwise you see a message telling you that no router interfaces are available, and the configuration screen is not displayed.

To display the page, click **IP Multicast > DVMRP > Interface Configuration** in the tree view.

Figure 12-20. DVMRP Interface Configuration



The **DVMRP Interface Configuration** page contains the following fields:

- **Interface** — Select the interface for which data is to be configured. You must configure at least one router interface before you configure a DVMRP interface.
- **Interface Mode** — Select Enable or Disable from the drop-down menu to set the administrative mode of the selected DVMRP routing interface.
- **Interface Metric** — Enter the DVMRP metric for the selected interface. This value is sent in DVMRP messages as the cost to reach this network. Valid values are from 1 to 31.

Downloaded from www.Manualslib.com manuals search engine

Configuring a DVMRP Interface

1. Open the **DVMRP Interface Configuration** page.
2. Select the interface to configure from the **Interface** field.
3. Modify the remaining fields as needed.
4. Click **Apply Changes**.

   The interface configuration is saved, and the device is updated.

Configuring a DVMRP Interface using the CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide:*

- DVMRP Commands

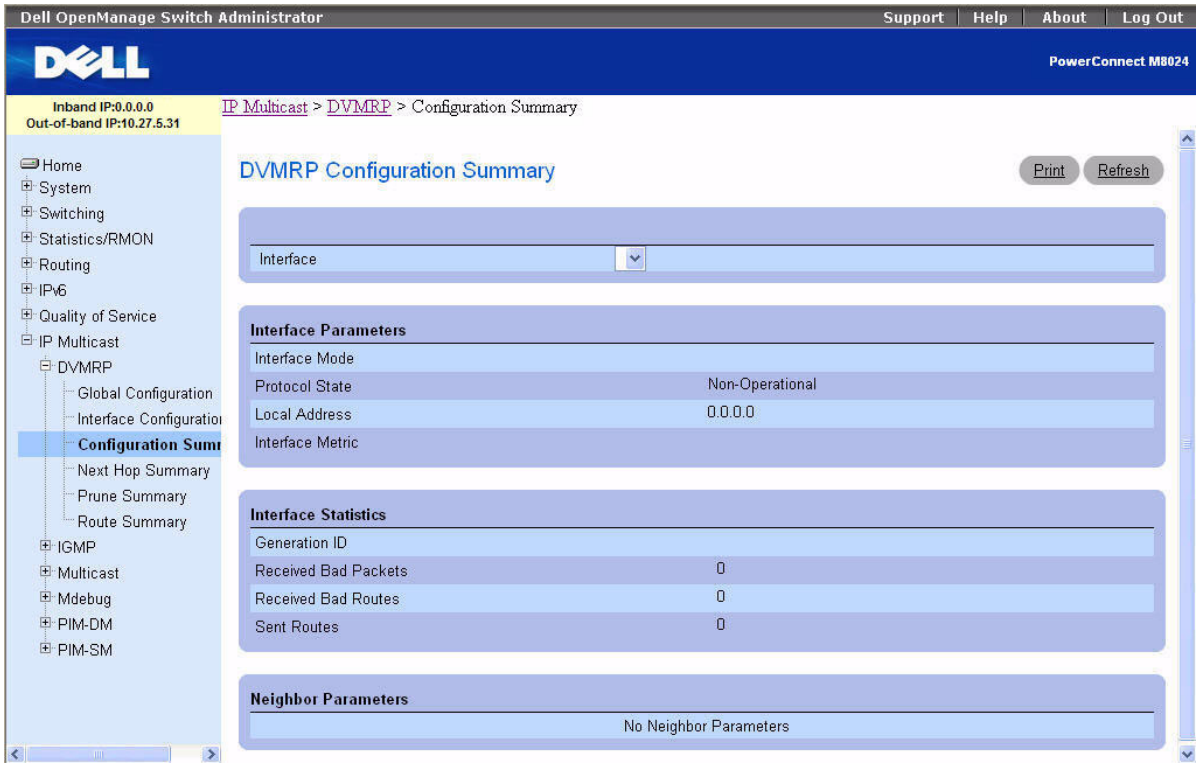
DVMRP Configuration Summary

Use the **DVMRP Configuration Summary** page to display or print the DVMRP configuration and data for a selected interface. You must configure at least one router interface before you can display data for a DVMRP interface. Otherwise you see a message telling you that no router interfaces are available, and the configuration summary screen is not displayed.

To display the page, click **IP Multicast > DVMRP > Configuration Summary** in the tree view.

Downloaded from www.Manualslib.com manuals search engine

Figure 12-21. DVMRP Configuration Summary



The **DVMRP Configuration Summary** page contains the following fields:

- **Interface** — Select the interface for which data is to be displayed. You must configure at least one router interface before you can display data for a DVMRP interface.

Interface Parameters

- **Interface Mode** — Displays the administrative mode of the selected DVMRP routing interface, either Enable or Disable.
- **Protocol State** — Displays the operational state of the DVMRP protocol on the selected interface, either Operational or Non-operational.
- **Local Address** — Displays the IP address used as a source address in packets sent from the selected interface.
- **Interface Metric** — Displays the metric used to calculate distance vectors for the selected interface.

Interface Statistics

- **Generation ID** — Displays the DVMRP generation ID used by the router for the selected interface. This value is reset every time an interface is (re)started and is placed in prune messages. A change in generation ID informs the neighbor routers that any previous information about this router should be discarded.
- **Received Bad Packets** — The number of invalid packets received on the selected interface.

Downloaded from www.Manualslib.com manuals search engine

- **Received Bad Routes** — The number of invalid routes received on the selected interface.
- **Sent Routes** — The number of routes sent on the selected interface.

Neighbor Parameters

- **Neighbor IP** — The IP address of the neighbor whose information is displayed.
- **State** — The state of the specified neighbor router on the selected interface, either active or down.
- **Neighbor Uptime** — The DVMRP uptime for the specified neighbor on the selected interface. This is the time since the neighbor entry was learned.
- **Neighbor Expiry Time** — The DVMRP expiry time for the specified neighbor on the selected interface. This is the time left before this neighbor entry ages out, and is not applicable if the neighbor router's state is down.
- **Generation ID** — The DVMRP generation ID for the specified neighbor on the selected interface.
- **Major Version** — The DVMRP Major Version for the specified neighbor on the selected interface.
- **Minor Version** — The DVMRP Minor Version for the specified neighbor on the selected interface.
- **Capabilities** — The DVMRP capabilities of the specified neighbor on the selected interface.
- **Received Routes** — The number of routes received for the specified neighbor on the selected interface.
- **Received Bad Packets** — The number of invalid packets received for the specified neighbor on the selected interface.
- **Received Bad Routes** — The number of invalid routes received for the specified neighbor on the selected interface.

Displaying DVMRP Configuration Summary using the CLI Command

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide:*

- DVMRP Commands

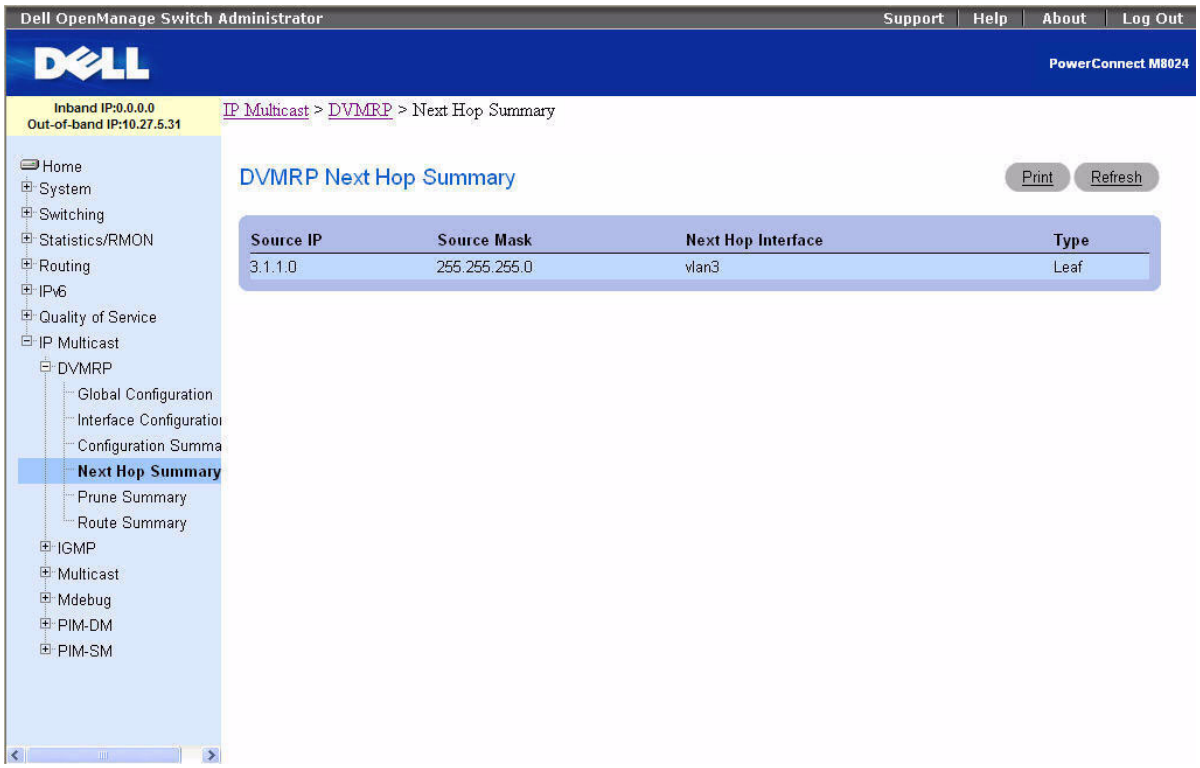
Downloaded from www.Manualslib.com manuals search engine

Next Hop Summary

Use the **Next Hop Summary** page to display or print the next hop summary by Source IP.

To display the page, click **IP Multicast > DVMRP > Next Hop Summary** in the tree view.

Figure 12-22. Next Hop Summary



The **Next Hop Summary** page displays the following fields:

- **Source IP** — Displays the IP address used with the source mask to identify the source network for this table entry.
- **Source Mask** — Displays the network mask used with the source IP address.
- **Next Hop Interface** — Displays the outgoing interface for this next hop.
- **Type** — Displays the next hop type. Leaf means that no downstream dependent neighbors exist on the outgoing interface. Otherwise, the type is Branch.

Displaying the Next Hop Summary using the CLI Command

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide:*

- DVMRP Commands

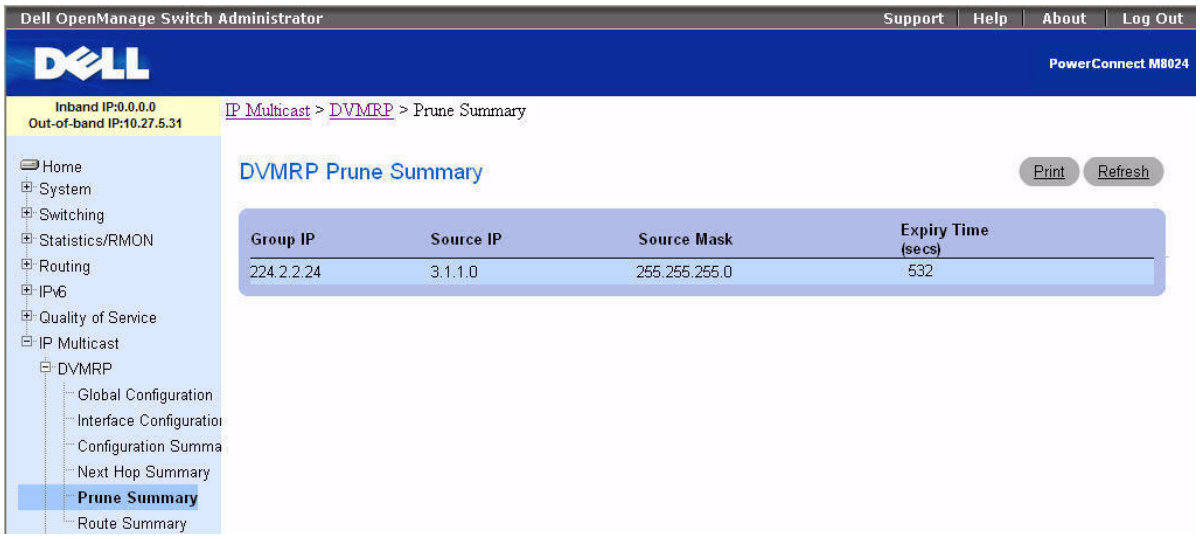
Downloaded from www.Manualslib.com manuals search engine

Prune Summary

Use the **Prune Summary** page to display or print the prune summary by Group IP.

To display the page, click **IP Multicast** > **DVMRP** > **Prune Summary** in the tree view.

Figure 12-23. Prune Summary



The **Prune Summary** page displays the following fields:

- **Group IP** — The group address which has been pruned.
- **Source IP** — The address of the source or source network which has been pruned.
- **Source Mask** — The subnet mask to be combined with the source IP address to identify the source or source network which has been pruned.
- **Expiry Time (secs)** — The amount of time remaining before this prune should expire at the upstream neighbor. If no prune messages have been received from downstream neighbors, this is set to value of the default prune lifetime timer, otherwise it is set to the smallest received value or the default timer, whichever is less.

Displaying the Prune Summary using the CLI Command

For information about the CLI command that performs this function, see the following chapter in the *CLI Reference Guide:*

- DVMRP Commands

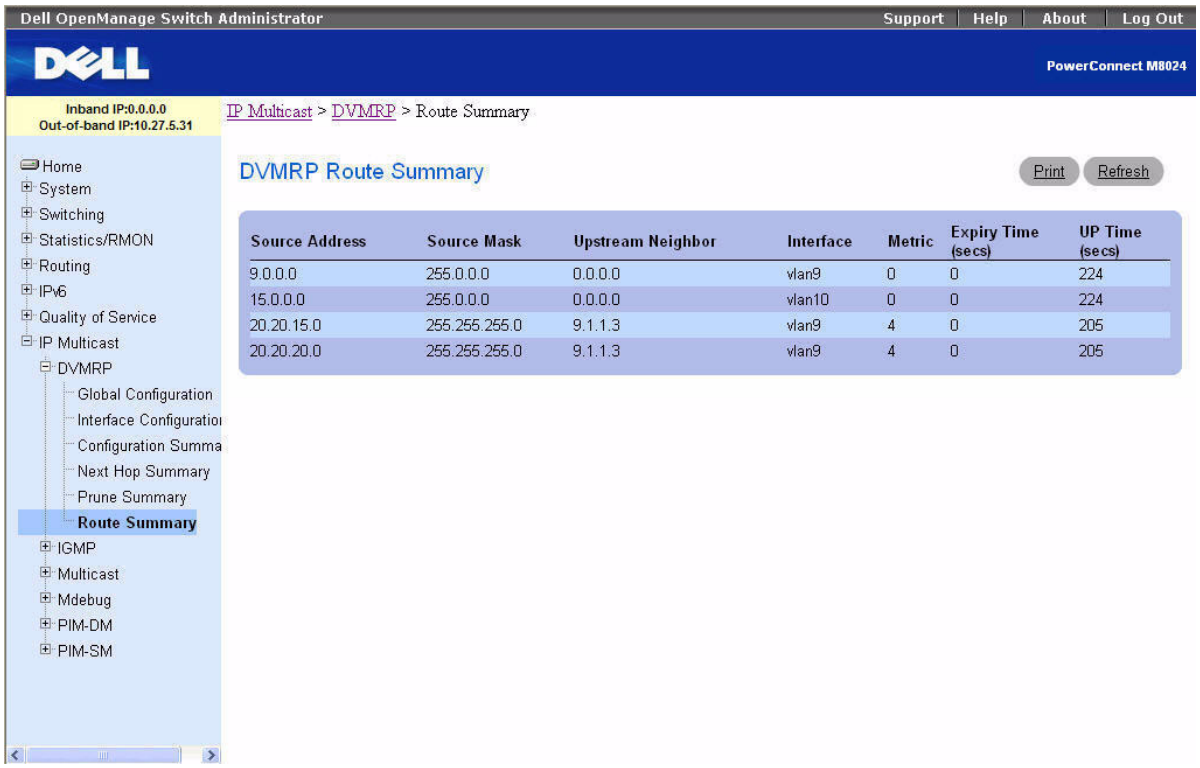
Downloaded from www.Manualslib.com manuals search engine

Route Summary

Use the **Route Summary** page to display or print the DVMRP route summary.

To display the page, click **IP Multicast** > **DVMRP** > **Route Summary** in the tree view.

Figure 12-24. Route Summary



Source Address	Source Mask	Upstream Neighbor	Interface	Metric	Expiry Time (secs)	UP Time (secs)
9.0.0.0	255.0.0.0	0.0.0.0	vlan9	0	0	224
15.0.0.0	255.0.0.0	0.0.0.0	vlan10	0	0	224
20.20.15.0	255.255.255.0	9.1.1.3	vlan9	4	0	205
20.20.20.0	255.255.255.0	9.1.1.3	vlan9	4	0	205

The **Route Summary** page displays the following fields:

- **Source Address** - The network address that is combined with the source mask to identify the sources for this entry.
- **Source Mask** — The subnet mask to be combined with the source address to identify the sources for this entry.
- **Upstream Neighbor** — The address of the upstream neighbor (for example, RPF neighbor) from which IP datagrams from these sources are received.
- **Interface** — The interface on which IP datagrams sent by these sources are received. A value of 0 typically means the route is an aggregate for which no next-hop interface exists.
- **Metric** — The distance in hops to the source subnet.
- **Expiry Time** — The minimum amount of time remaining before this entry is aged out.
- **Up Time** — The time since the route represented by this entry was learned by the router.

Downloaded from www.Manualslib.com manuals search engine

Displaying the DVMRP Route Summary using the CLI Command

For information about the CLI command that performs this function, see the following chapter in the *CLI Reference Guide:*

- DVMRP Commands

Internet Group Management Protocol

The Internet Group Management Protocol (IGMP) is used by IPv4 systems (hosts and routers) to report their IP multicast group memberships to any neighboring multicast routers. The PowerConnect M6220/M6348/M8024 performs the multicast router role of the IGMP protocol, which means it collects the membership information needed by the active multicast routing. The currently supported multicast routing protocols in the PowerConnect M6220/M6348/M8024 are DVMRP, PIM-DM, and PIM-SM.

The PowerConnect M6220/M6348/M8024 supports IGMP Version 3. Version 3 adds support for source filtering, which is the ability for a system to report interest in receiving packets only from specific source addresses, as required to support Source-Specific Multicast [SSM], or from all but specific source addresses, sent to a particular multicast address. Version 3 is designed to be interoperable with Versions 1 and 2.

The **IGMP** menu page contains links to web pages that define and display IGMP parameters and data. To display this page, click **IP Multicast > IGMP** in the tree view.

Following are the web pages accessible from this menu page:

- IGMP Global Configuration
- Routing Interface
- Proxy Interface

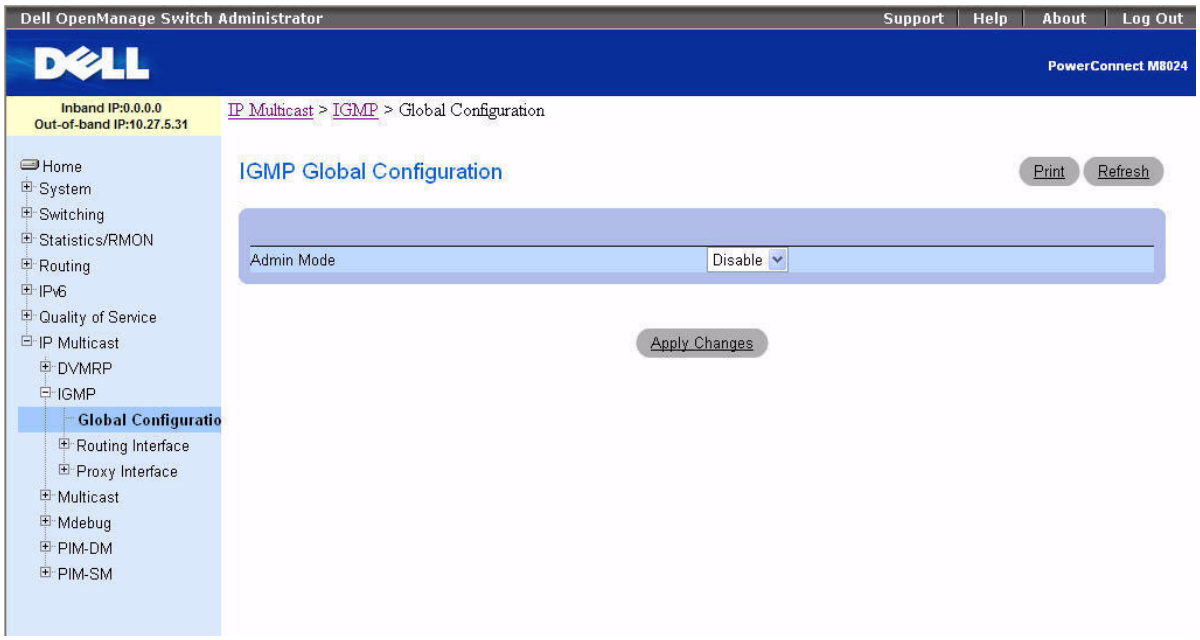
Downloaded from www.Manualslib.com manuals search engine

IGMP Global Configuration

Use the **IGMP Global Configuration** page to set IGMP on the system to active or inactive.

To display the page, click **IP Multicast > IGMP > Global Configuration** in the tree view.

Figure 12-25. IGMP Global Configuration



The **IGMP Global Configuration** page contains the following field:

- **Admin Mode** — Select Enable or Disable from the drop-down menu to set the administrative status of IGMP in the router to active or inactive. The default is Disable.

Setting the IGMP Mode

1. Open the **IGMP Global Configuration** page.
2. Set **Admin Mode** to Enable or Disable, to turn IGMP on or off.
3. Click **Apply Changes**.

   The IGMP configuration is saved, and the device is updated.

Setting IGMP Mode using the CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide:*

- IGMP Commands

Downloaded from www.Manualslib.com manuals search engine

Routing Interface

The **Routing Interface** menu page contains links to web pages that configure and display IGMP routing parameters and data. To display this page, click **IP Multicast > IGMP > Routing Interface** in the tree view. Following are the web pages accessible from this menu page:

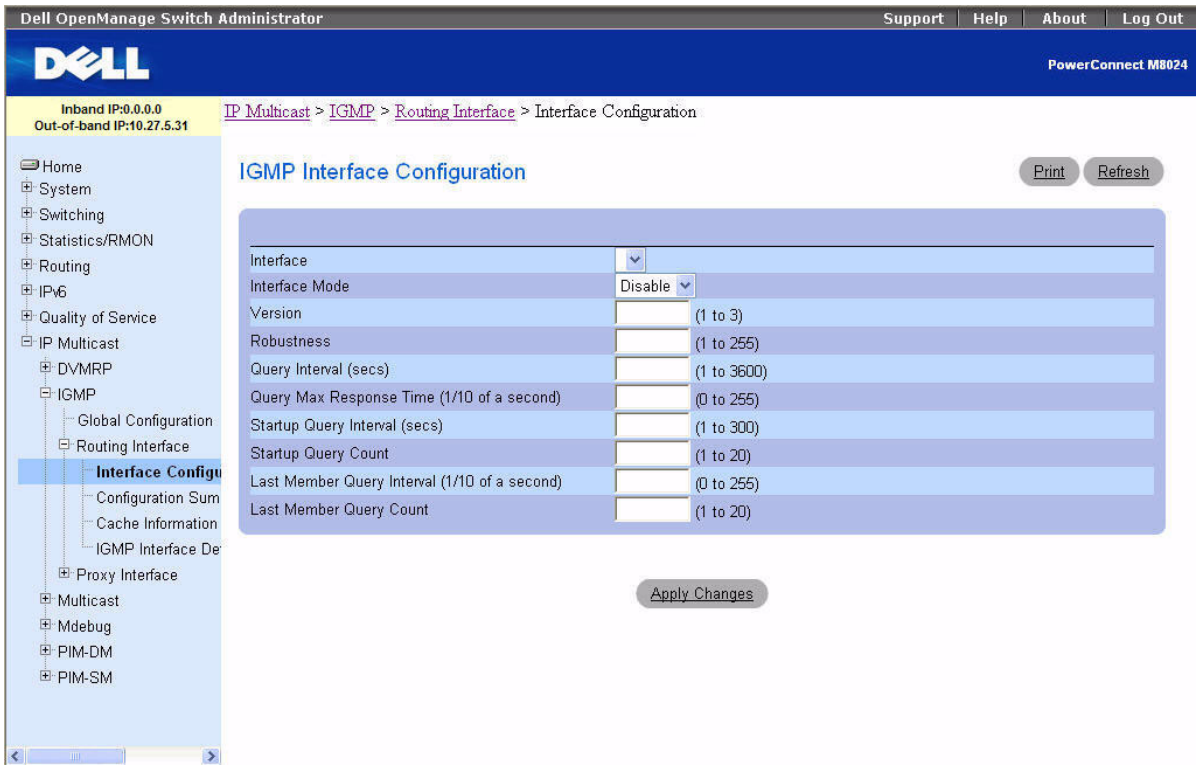
- IGMP Interface Configuration
- IGMP Configuration Summary
- IGMP Cache Information
- IGMP Interface Detailed Membership Info

IGMP Interface Configuration

Use the **IGMP Interface Configuration** page to configure and/or display router interface parameters. You must configure at least one valid routing interface before you can access this page and configure IP Multicast IGMP.

To display the page, click **IP Multicast > IGMP > Routing Interface > Interface Configuration** in the tree view.

Figure 12-26. IGMP Interface Configuration



Downloaded from www.Manualslib.com manuals search engine

The **IGMP Interface Configuration** page contains the following fields:

- **Interface** — Select the interface for which data is to be displayed or configured from the drop-down menu.
- **Interface Mode** — Select Enable or Disable from the drop-down menu to set the administrative status of IGMP on the selected interface. The default is Disable.
- **Version** — Enter the version of IGMP you want to configure on the selected interface. Valid values are 1 to 3, and the default value is 3. This field is configurable only when IGMP interface mode is enabled.
- **Robustness** — Enter the robustness value. This variable allows tuning for the expected packet loss on a subnet. If you expect the subnet to be lossy, you should enter a higher number for this parameter. IGMP is robust to (robustness variable-1) packet losses. Valid values are from 1 to 255. The default value is 2.
- **Query Interval (secs)** — Enter the frequency in seconds at which IGMP host-query packets are to be transmitted on this interface. Valid values are from 1 to 3600. The default value is 125.
- **Query Max Response Time (1/10 of a second)** — Enter the maximum query response time to be advertised in IGMPv2 queries on this interface, in tenths of a second. The default value is 100. Valid values are from 0 to 255.
- **Startup Query Interval (secs)** — Enter the number of seconds between the transmission of startup queries on the selected interface. The valid values are from 1 to 300. The default value is 31.
- **Startup Query Count** — Enter the number of queries to be sent on startup. The valid values are from 1 to 20. The default value is 2.
- **Last Member Query Interval (1/10 of a second)** — Enter the last member query interval in tenths of a second. This is the maximum response time to be inserted into group-specific queries sent in response to leave group messages, and is also the amount of time between group-specific query messages. Valid values are from 0 to 255. The default value is 10. This value is not used for IGMP version 1.
- **Last Member Query Count** — Enter the number of queries to be sent on receiving a leave group report. Valid values are from 1 to 20. The default value is 2.

Configuring an IGMP Routing Interface

1. Open the **IGMP Interface Configuration** page.
2. Select the interface to configure from the **Interface** field.
3. Modify the remaining fields as needed.
4. Click **Apply Changes**.

   The interface configuration is saved, and the device is updated.

Configuring an IGMP Routing Interface using the CLI Command

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide:*

- IGMP Commands

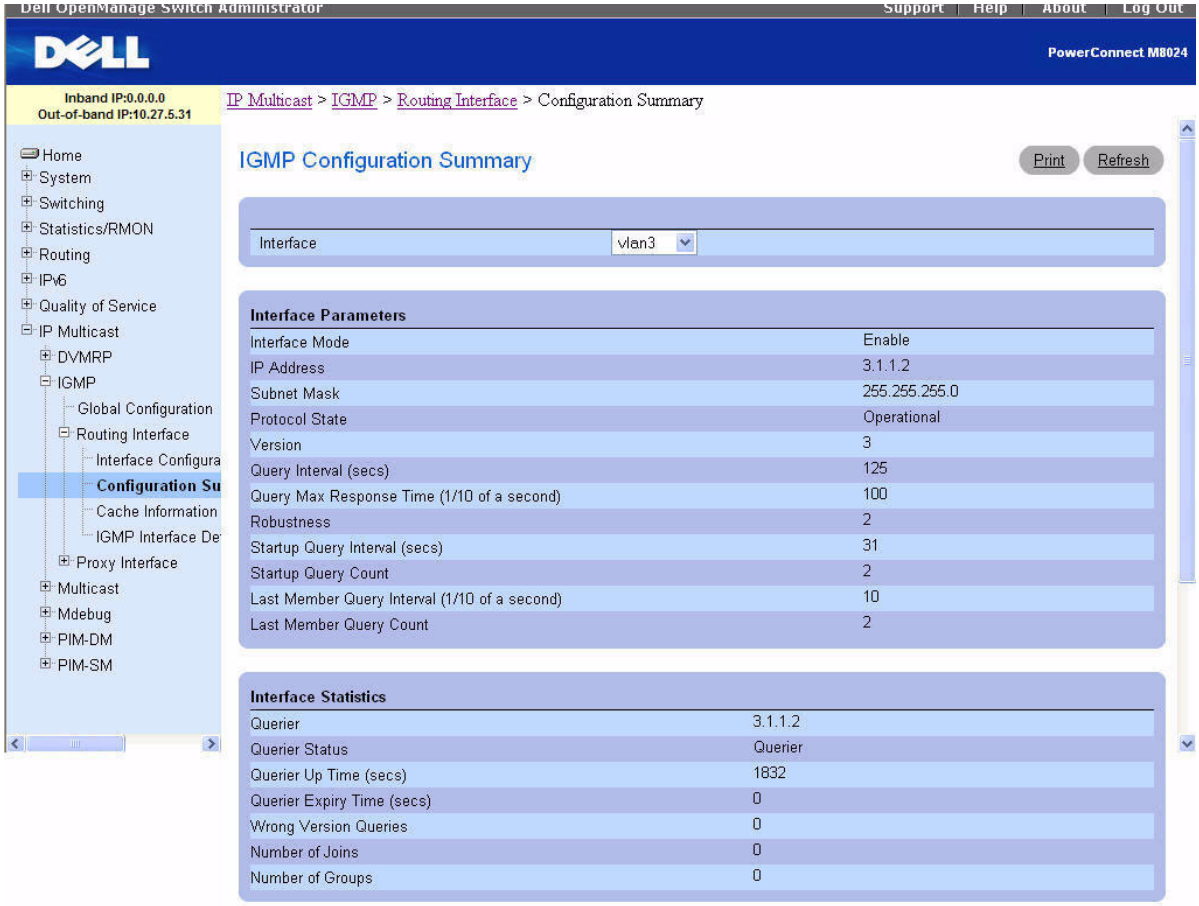
Downloaded from www.Manualslib.com manuals search engine

IGMP Configuration Summary

Use the **IGMP Configuration Summary** page to display IGMP routing parameters and data. You must configure at least one IGMP router interface to access this page.

To display the page, click **IP Multicast > IGMP > Routing Interface > Configuration Summary** in the tree view.

Figure 12-27. IGMP Configuration Summary



The **IGMP Configuration Summary** page displays the following fields:

- **Interface** — Select the interface for which data is to be displayed.
- Interface Parameters
- **Interface Mode** — The administrative status of IGMP on the selected interface.
- **IP Address** — The IP address of the selected interface.
- **Subnet Mask** — The subnet mask for the IP address of the selected interface.
- **Protocol State** — The operational state of IGMP on the selected interface.

Downloaded from www.Manualslib.com manuals search engine

- **Version** — The version of IGMP configured on the selected interface.
- **Query Interval (secs)** — The frequency at which IGMP host-query packets are transmitted on the selected interface.
- **Query Max Response Time (1/10 of a second)** — The maximum query response time advertised in IGMPv2 queries sent from the selected interface.
- **Robustness** — The robustness parameter for the selected interface. This variable allows tuning for the expected packet loss on a subnet. If a subnet is expected to be lossy, the robustness variable may be increased. IGMP is robust to (robustness variable-1) packet losses.
- **Startup Query Interval (secs)** — The interval at which startup queries are sent on the selected interface.
- **Startup Query Count** — The number of queries to be sent on startup.
- **Last Member Query Interval (1/10 of a second)** — The last member query interval is the maximum response time inserted into group-specific queries sent in response to leave group messages, and is also the amount of time between group-specific query messages. This value may be tuned to modify the leave latency of the network. A reduced value results in reduced time to detect the loss of the last member of a group. This value is not used for IGMP version 1.
- **Last Member Query Count** — The number of queries to be sent on receiving a leave group report.
- Interface Statistics
- **Querier** — The address of the IGMP querier on the IP subnet to which the selected interface is attached.
- **Querier Status** — Indicates whether the selected interface is in querier or non querier mode.
- **Querier Up Time (secs)** — The time in seconds since the IGMP interface querier was last changed.
- **Querier Expiry Time (secs)** — The time in seconds remaining before the other querier present timer expires. If the local system is the querier, this is zero.
- **Wrong Version Queries** — The number of queries that have been received on the selected interface with an IGMP version that does not match the IGMP version configured for the interface, over the lifetime of the entry. IGMP requires that all routers on a LAN be configured to run the same version of IGMP. Therefore, a configuration error is indicated if any queries are received with the wrong version number.
- **Number of Joins** — The number of times a group membership has been added on the selected interface; that is, the number of times an entry for this interface has been added to the cache table. This gives an indication of the amount of IGMP activity on the interface.
- **Number of Groups** — The current number of entries for the selected interface in the cache table.

Displaying the IGMP Routing Configuration using the CLI Command

For information about the CLI command that performs this function, see the following chapter in the *CLI Reference Guide:*

- IGMP Commands

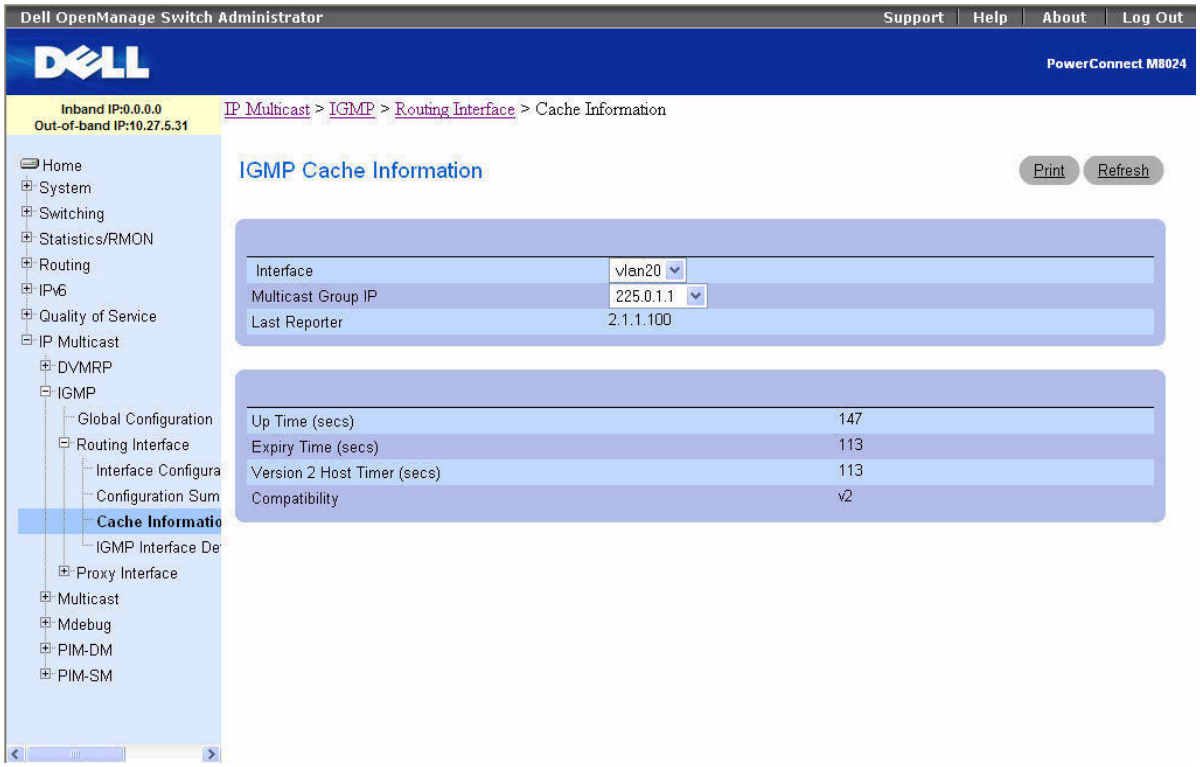
Downloaded from www.Manualslib.com manuals search engine

IGMP Cache Information

Use the **IGMP Cache Information** page to display cache parameters and data for an IP multicast group address. You must configure at least one IGMP router interface to access this page. Also, group membership reports must have been received on the selected interface for data to display here.

To display the page, click **IP Multicast > IGMP > Routing Interface > Cache Information** in the tree view.

Figure 12-28. IGMP Cache Information



The **IGMP Cache Information** page displays the following fields:

- **Interface** — Select the interface for which data is to be displayed.
- **Multicast Group IP** — Select the IP multicast group address for which data is to be displayed. If no group membership reports have been received on the selected interface you cannot make this selection, and none of the data on this page displays.
- **Last Reporter** — The IP address of the source of the last membership report received for the IP Multicast group address on the selected interface.
- **Up Time** — The time elapsed since this entry was created.
- **Expiry Time** — The minimum amount of time remaining before this entry ages out.

Downloaded from www.Manualslib.com manuals search engine

- **Version 1 Host Timer** — The time remaining until the local router assumes that there are no longer any IGMP version 1 members on the IP subnet attached to this interface. When an IGMPv1 membership report is received, this timer is reset to the group membership timer. While this timer is non-zero, the local router ignores any IGMPv2 leave messages for this group that it receives on the selected interface. This field is displayed only if the interface is configured for IGMP version 1.
- **Version 2 Host Timer** — The time remaining until the local router assumes that there are no longer any IGMP version 2 members on the IP subnet attached to this interface. When an IGMPv2 membership report is received, this timer is reset to the group membership timer. While this timer is non-zero, the local router ignores any IGMPv1 and IGMPv3 leave messages for this group that it receives on the selected interface. This field is displayed only if the interface is configured for IGMP version 2.
- **Compatibility** — This parameter shows group compatibility mode (v1, v2 and v3) for this group on the specified interface.
- **Filter Mode** — The source filter mode (Include/Exclude/NA) for the specified group on this interface. When NA mode is active the field is blank.

Displaying Cache Information using the CLI Command

For information about the CLI command that performs this function, see the following chapter in the *CLI Reference Guide:*

- IGMP Commands

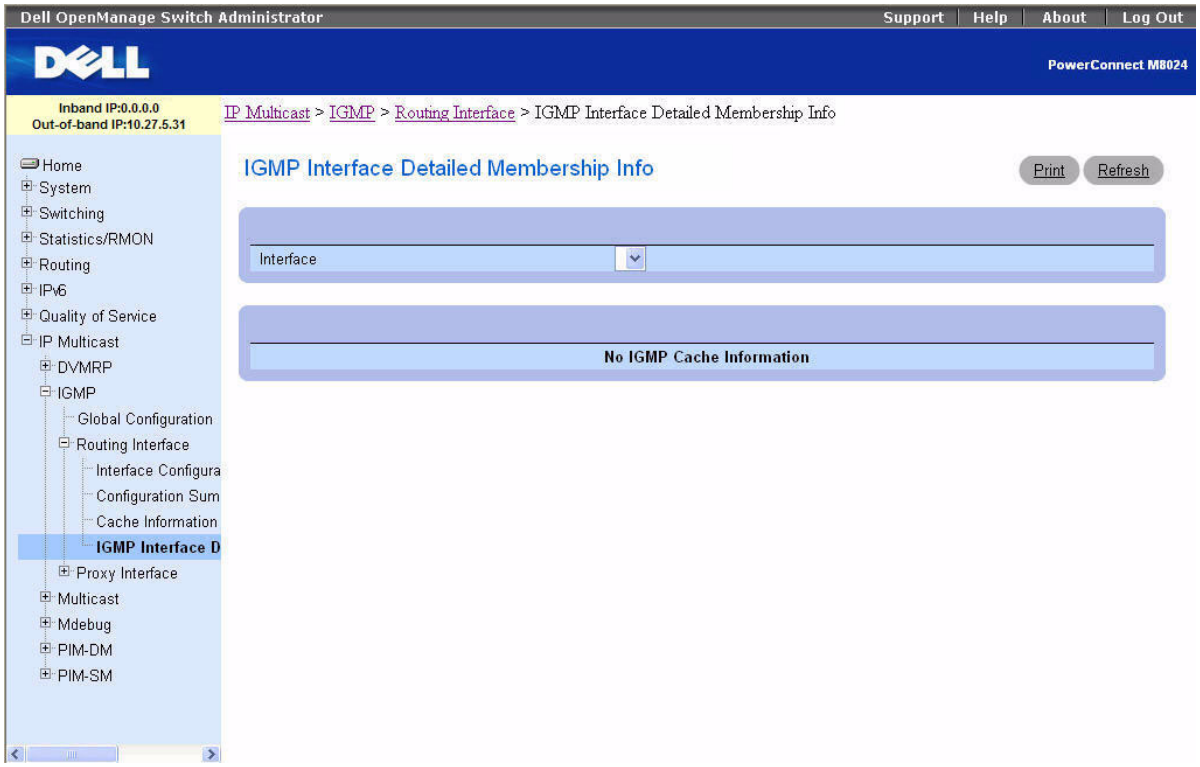
Downloaded from www.Manualslib.com manuals search engine

IGMP Interface Detailed Membership Info

Use the **IGMP Interface Detailed Membership Info** page to display detailed membership information for an interface. You must configure at least one IGMP router interface to access this page. Also, group membership reports must have been received on the selected interface for data to display here.

To display the page, click **IP Multicast > IGMP > Routing Interface > IGMP Interface Detailed Membership Info** in the tree view.

Figure 12-29. IGMP Interface Detailed Membership Info



The **IGMP Interface Detailed Membership Info** page displays the following fields:

- **Interface** — Select the interface for which data is to be displayed.
- **Multicast Group IP** — Select the IP multicast group address for which data is to be displayed. If no group membership reports have been received on the selected interface, you cannot make this selection, and none of the remaining fields are displayed.
- **Interface** — The interface on which multicast packets are forwarded.
- **Group Compatibility Mode** — The group compatibility mode (v1, v2 and v3) for this group on the specified interface.
- **Source Filter Mode** — The source filter mode (Include/Exclude/NA) for the specified group on this interface.

Downloaded from www.Manualslib.com manuals search engine

- **Source Hosts** — The source addresses which are members of this multicast address.
- **Expiry Time** — The expiry time interval against each source address which are members of this multicast group. This is the amount of time after which the specified source entry is aged out.

Displaying IGMP Interface Detailed Membership

1. Open the **IGMP Interface Detailed Membership Info** page.
2. Select the interface to display from the **Interface** drop-down menu.
3. Select the desired **Multicast Group IP**.

   Detailed membership information for this interface and multicast group IP displays.

Displaying IGMP Interface Detailed Membership using the CLI Command

For information about the CLI command that performs this function, see the following chapter in the *CLI Reference Guide:*

- IGMP Commands

Proxy Interface

The purpose of IGMP Proxy is to enable a multicast router to learn multicast group membership information and be able to forward multicast packets based upon the group membership information. The IGMP Proxy is capable of functioning only in certain topologies that do not require Multicast Routing Protocols (i.e. DVMRP, PIM-DM, and PIM-SM) and that have a tree-like topology, as there is no support for features like spanning tree to correct packet route loops.

The **Proxy Interface** menu page contains links to web pages that define and display Proxy Interface parameters and data. To display this page, click **IP Multicast > IGMP > Proxy Interface** in the tree view. Following are the web pages accessible from this menu page:

- IGMP Proxy Interface Configuration
- IGMP Proxy Configuration Summary
- IGMP Proxy Interface Membership Info
- IGMP Proxy Interface Membership Info Detailed

IGMP Proxy Interface Configuration

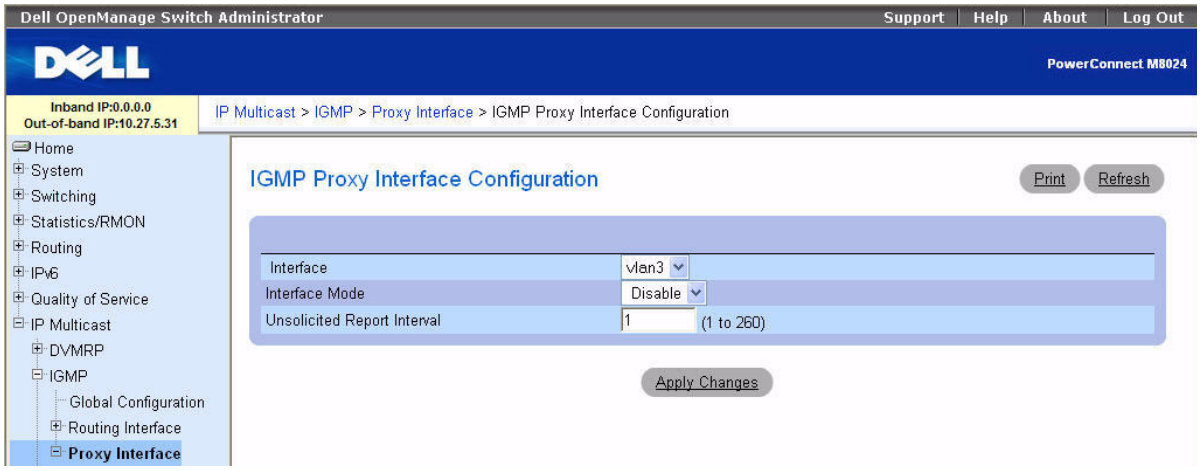
The IGMP Proxy is used by IGMP Router (IPv4 system) to enable the system to issue IGMP host messages on behalf of hosts that the system discovered through standard IGMP router interfaces. Thus, this feature acts as proxy to all hosts residing on its router interfaces.

Use the **IGMP Proxy Interface Configuration** page to configure IGMP proxy for an interface. You must have configured at least one router interface before configuring or displaying data for an IGMP proxy interface, and it should not be an IGMP routing interface.

To display the page, click **IP Multicast > IGMP > Proxy Interface > Interface Configuration** in the tree view.

Downloaded from www.Manualslib.com manuals search engine

Figure 12-30. IGMP Proxy Interface Configuration



The **IGMP Proxy Interface Configuration** page contains the following fields:

- **Interface** — Select the port for which data is to be displayed or configured from the drop-down menu. You must have configured at least one router interface before configuring or displaying data for an IGMP Proxy interface and it should not be a IGMP routing interface. This field is configurable only when interface mode is disabled.
- **Interface Mode** — Select Enable or Disable from the drop-down menu to set the administrative status of IGMP Proxy on the selected interface. The default is Disable. Routing, IGMP, and Multicast global admin modes should be enabled to enable IGMP Proxy interface mode.
- **Unsolicited Report Interval** — Enter the unsolicited time interval value in seconds. The Unsolicited Report Interval is the time between repetitions of a host's initial report of membership in a group. Valid values are from 1 to 260. The default value is 1.

Configuring IGMP Proxy Interface

1. Open the **IGMP Proxy Interface Configuration** page.
2. Select the interface to display from the **Interface** drop-down menu.
3. Modify the remaining fields as needed.
4. Click **Apply Changes**.

   The proxy interface configuration is saved, and the device is updated.

Configuring IGMP Proxy Interface using the CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide:*

- IGMP Proxy Commands

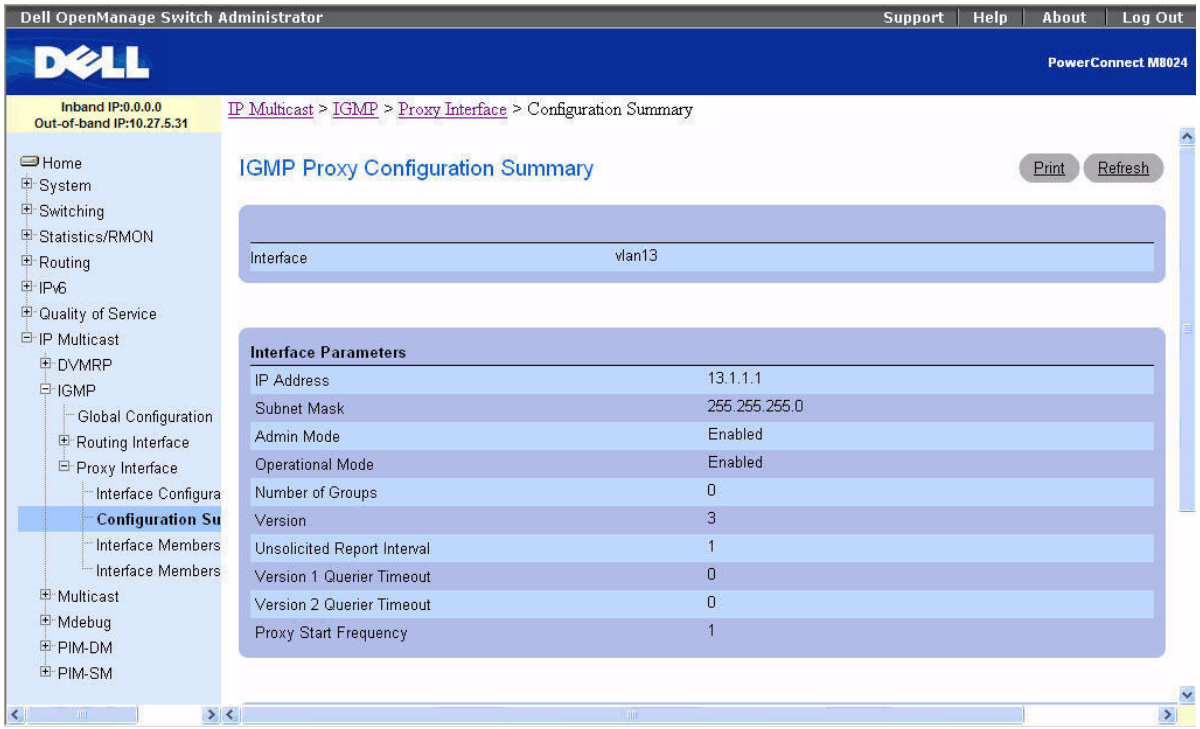
Downloaded from www.Manualslib.com manuals search engine

IGMP Proxy Configuration Summary

Use the **IGMP Proxy Configuration Summary** page to display proxy interface configurations by interface. You must have configured at least one router interface configured before data displays on this page.

To display the page, click **IP Multicast > IGMP > Proxy Interface > Configuration Summary** in the tree view.

Figure 12-31. IGMP Proxy Configuration Summary



The **IGMP Proxy Configuration Summary** page displays the following fields:

- **Interface** — Displays the interface on which IGMP proxy is enabled. There can be only one IGMP Proxy interface.
- **IP Address** — The IP address of the IGMP Proxy interface.
- **Subnet Mask** — The subnet mask for the IP address of the IGMP Proxy interface.
- **Admin Mode** — The administrative status of IGMP Proxy on the selected interface.
- **Operational Mode** — The operational state of IGMP Proxy interface.
- **Number of Groups** — The current number of multicast group entries for the IGMP Proxy interface in the cache table.
- **Version** — The version of IGMP configured on the IGMP Proxy interface.

Downloaded from www.Manualslib.com manuals search engine

- **Unsolicited Report Interval** — The Unsolicited Report Interval is the time between repetitions of a host's initial report of membership in a group. Default: 1 second.
- **Version 1 Querier Timeout** — The older IGMP version 1 querier timeout value in seconds. The Older Version Querier Interval is the time-out for transitioning a host back to IGMPv3 mode once an older version query is heard. When an older version query is received, hosts set their Older Version Querier Present Timer to Older Version Querier Interval.
- **Version 2 Querier Timeout** — The older IGMP version 2 querier timeout value in seconds.
- **Proxy Start Frequency** — The number of times the proxy was brought up.
- **Proxy Interface Statistics** — The Queries Received, Reports Received/Sent, Leaves Received/Sent

Displaying IGMP Proxy Interface Configurations using the CLI Command

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide:*

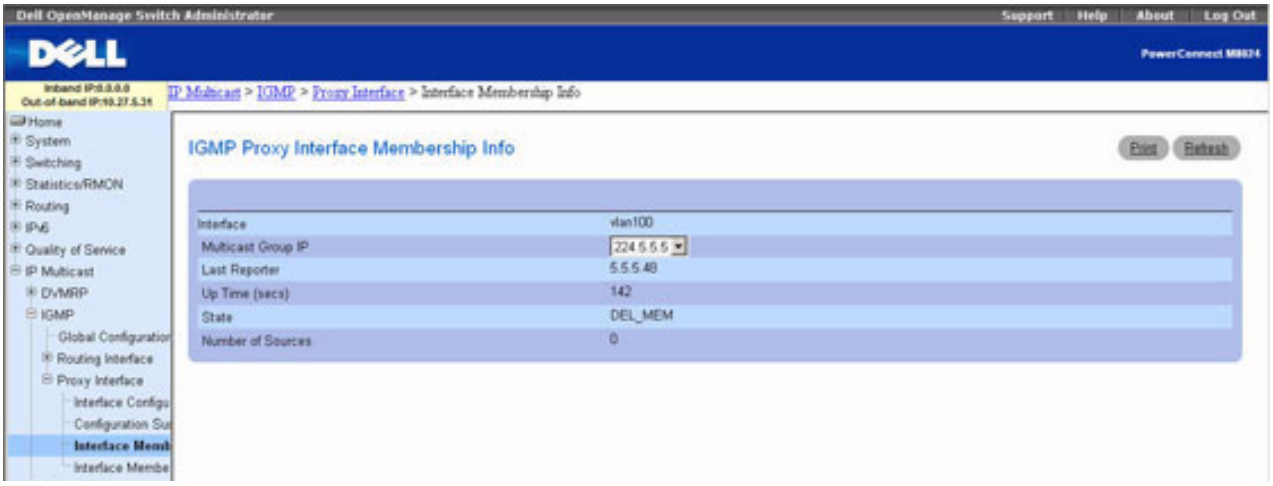
- IGMP Proxy Commands

IGMP Proxy Interface Membership Info

Use the **IGMP Proxy Interface Membership Info** page to display interface membership data for a specific IP multicast group address. You must have configured at least one router interface before you can display interface membership information, and it should not be an IGMP routing interface. Also, if no group membership reports have been received on the selected interface, no data displays on this page.

To display the page, click **IP Multicast > IGMP > Proxy Interface > Interface Membership Info** in the tree view.

Figure 12-32. IGMP Proxy Interface Membership Info



Downloaded from www.Manualslib.com manuals search engine

The **IGMP Proxy Interface Membership Info** page displays the following fields:

- **Interface** — Displays the interface on which IGMP proxy is enabled.
- **Multicast Group IP** — Select the IP multicast group address for which data is to be displayed. If no group membership reports have been received on the selected interface you cannot make this selection, and none of the following data displays.
- **Last Reporter** — The IP address of the source of the last membership report received for the IP Multicast group address on the IGMP Proxy interface.
- **Up Time (secs)** — The time elapsed since this entry was created.
- **State** — The state of the host entry. A Host can be in one of the state. Non-member state - does not belong to the group on the interface. Delaying member state - host belongs to the group on the interface and report timer running. The report timer is used to send out the reports. Idle member state - host belongs to the group on the interface and no report timer running.
- **Number of Sources** — The number of source hosts present in the selected multicast group.

Displaying IGMP Proxy Interface Membership Info using the CLI Command

For information about the CLI command that performs this function, see the following chapter in the *CLI Reference Guide:*

- IGMP Proxy Commands

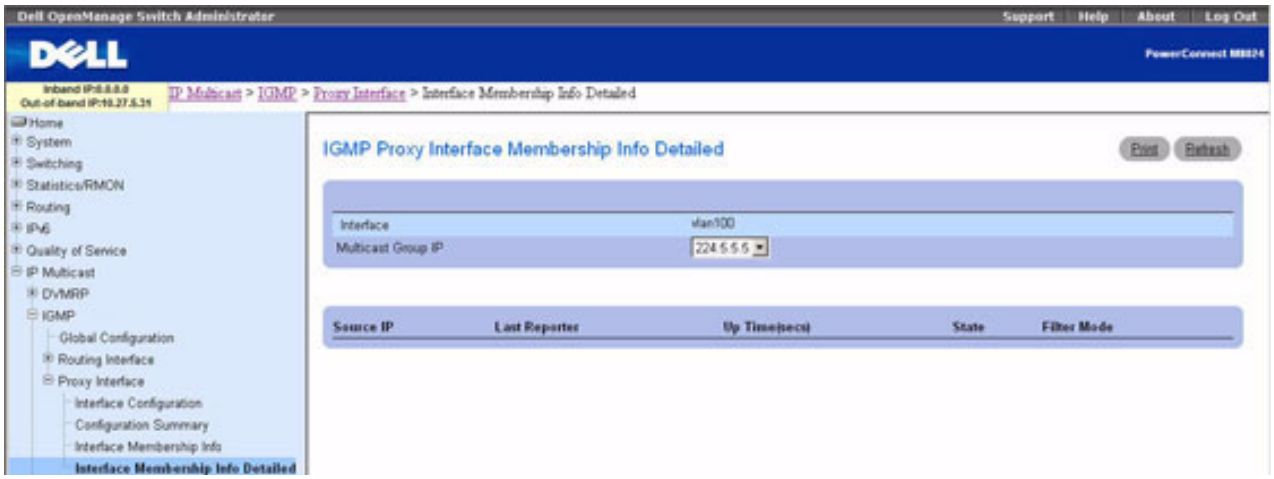
Downloaded from www.Manualslib.com manuals search engine

IGMP Proxy Interface Membership Info Detailed

Use the **IGMP Proxy Interface Membership Info Detailed** page to display detailed interface membership data. You must have configured at least one router interface before you can display detailed interface membership information, and it should not be an IGMP routing interface. Also, if no group membership reports have been received on the selected interface you cannot display data.

To display the page, click **IP Multicast > IGMP > Proxy Interface > Interface Membership Info Detailed** in the tree view.

Figure 12-33. IGMP Proxy Interface Membership Info Detailed



The **IGMP Proxy Interface Membership Info Detailed** page contains the following fields:

- **Interface** — Select the interface for which data is to be displayed.
- **Multicast Group IP** — Select the IP multicast group address for which data is to be displayed. If no group membership reports have been received on the selected interface, you are not able to make this selection, and none of the non-configurable data is displayed.
- **Source IP** — This parameter shows source addresses that are members of this multicast address.
- **Last Reporter** — The IP address of the source of the last membership report received for the selected interface's IP Multicast group address.
- **Up Time (secs)** — Displays the up time since the entry was created in the cache table.
- **State** — The state of the host entry. A host can be in one of the following states:
  - **Non-member State** — Does not belong to the group on the interface.
  - **Delaying Member State** — Host belongs to the group on the interface and report timer is running. The report timer is used to send out the reports.
  - **Idle Member State** — Host belongs to the group on the interface and no report timer is running.
- **Filter Mode** — The group filter mode (Include/Exclude/None) for the specified group on the IGMP Proxy interface.

Downloaded from www.Manualslib.com manuals search engine

Displaying Detailed IGMP Proxy Interface Membership Info

1. Open the **IGMP Proxy Interface Membership Info Detailed** page.
2. Select the interface to display from the **Interface** drop-down menu.
3. Select the desired **Multicast Group IP**.

   Detailed membership data for this interface and multicast group IP displays.

Displaying Detailed IGMP Proxy Interface Membership Info using the CLI Command

For information about the CLI command that performs this function, see the following chapter in the *CLI Reference Guide:*

- IGMP Proxy Commands

Protocol Independent Multicast-Dense Mode

Protocol Independent Multicast-Dense Mode (PIM-DM) protocol is a simple, protocol-independent multicast routing protocol. It uses an existing Unicast routing table and a Join/Prune/Graft mechanism to build a tree. PIM-DM creates source-based shortest-path distribution trees that make use of RPF. It cannot be used to build a shared distribution tree, as is the case in PIM-SM. PIM-DM assumes that when a sender starts sending data, all downstream routers and hosts want to receive a multicast datagram. PIM-DM initially floods multicast traffic throughout the network. Routers that do not have any downstream neighbors prune back the unwanted traffic. In addition to PRUNE messages, PIM-DM makes use of graft and assert messages. Graft messages are used whenever a new host wants to join the group. Assert messages are used to shutoff duplicate flows on the same multi-access network.

There are two versions of PIM-DM. Version 2 doesn't use the IGMP message; instead, it uses a message that is encapsulated in IP package, with protocol number 103. In Version 2, Hello message is introduced in place of query message.

PIM-DM is appropriate for:

- Densely distributed receivers
- Few senders -to- many receivers (due to frequent flooding)
- High volume of multicast traffic
- Constant stream of traffic

The **PIM-DM** menu page contains links to web pages that define and display **PIM-DM** parameters and data. To display this page, click **IP Multicast > PIM-DM** in the tree view.

Following are the web pages accessible from this menu page:

- PIM-DM Global Configuration
- PIM-DM Global Status
- PIM-DM Interface Configuration
- PIM-DM Interface Summary

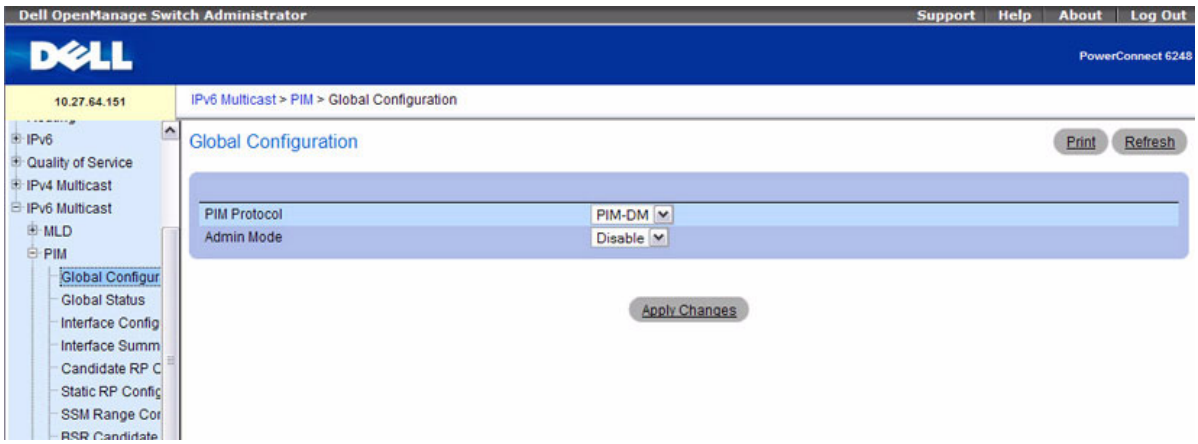
Downloaded from www.Manualslib.com manuals search engine

PIM-DM Global Configuration

Use the **PIM-DM Global Configuration** page to configure the administrative status of PIM-DM or PIM-SM on the switch.

To display the page, click **IPv4 Multicast > PIM > Global Configuration** or **IPv6 Multicast > PIM > Global Configuration** in the navigation tree.

Figure 12-34. PIM Global Configuration



The **PIM Global Configuration** page contains the following fields:

- **PIM Protocol** — Select PIM-DM or PIM-SM. Only one PIM protocol can be enabled on the switch at a time. If you select PIM-SM, additional fields appear.
- **Admin Mode** — Select Enable or Disable from the drop-down menu to set the administrative status of PIM on the system. The default is Disable.
- **Data Threshold Rate** — If PIM-SM is selected as the protocol, enter the minimum source data rate in K bits/second above which the last-hop router switches to a source-specific shortest path tree. The valid values are from 0 to 2000 K bits/sec. The default value is 0. This field is not available for PIM-DM.

Register Threshold Rate — If PIM-SM is selected as the protocol, enter the minimum source data rate in K bits/second above which the Rendezvous Point router switches to a source-specific shortest path tree. The valid values are from 0 to 2000 K bits/sec. The default value is 0. This field is not available for PIM-DM.

Configuring PIM-DM

1. Open the **PIM-DM Global Configuration** page.
2. Set **Admin Mode** to Enable or Disable, to turn PIM-DM on or off.
3. Click **Apply Changes**.

   The PIM-DM configuration is saved, and the device is updated.

Downloaded from www.Manualslib.com manuals search engine

Configuring PIM-DM using the CLI Command

For information about the CLI command that performs this function, see the following chapter in the *CLI Reference Guide:*

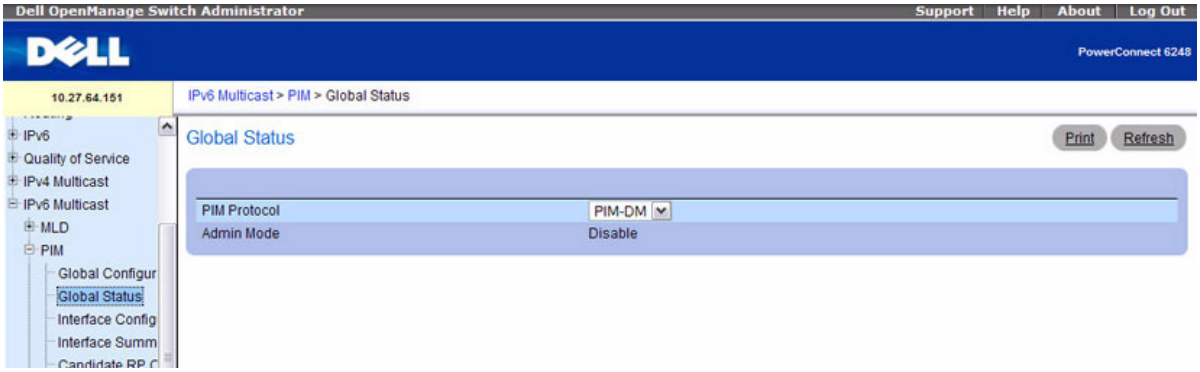
- PIM-DM Commands

PIM-DM Global Status

Use the **PIM-DM Global Status** page to view the administrative status of PIM-DM or PIM-SM on the switch.

To display the page, click **IPv4 Multicast > PIM-DM > Global Status** or **IPv6 Multicast > PIM > Global Status** in the tree view.

Figure 12-35. PIM Global Status



The **PIM Global Status** page contains the following fields:

- PIM Protocol — Select PIM-DM or PIM-SM. Only one PIM protocol can be enabled on the switch at a time. If you select PIM-SM, additional fields appear.
- **Admin Mode** — Displays the administrative status of the selected PIM protocol on the system.
- **Data Threshold Rate** — If PIM-SM is selected as the protocol, shows the minimum source data rate in Kbps above which the last-hop router switches to a source-specific shortest path tree.
- **Register Threshold Rate** — If PIM-SM is selected as the protocol, shows the minimum source data rate in Kbps above which the Rendezvous Point router switches to a source-specific shortest path tree.

Viewing Global PIM Settings using the CLI Command

For information about the CLI command that performs this function, see the following chapter in the *CLI Reference Guide:*

- PIM-DM or PIM-SM Commands

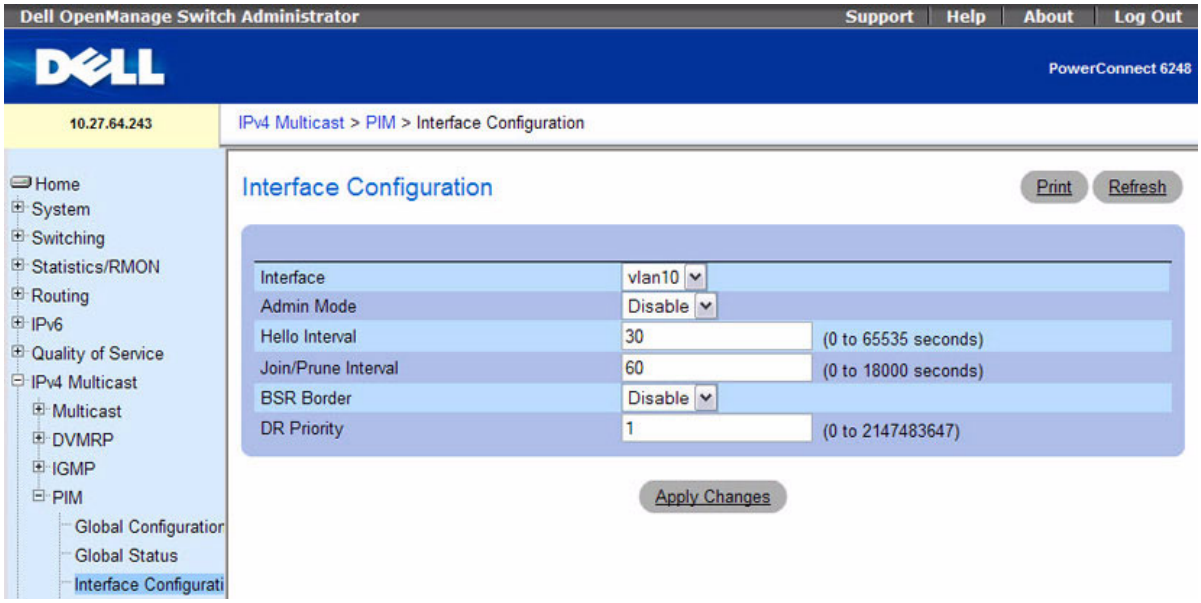
Downloaded from www.Manualslib.com manuals search engine

PIM-DM Interface Configuration

Use the **PIM-DM Interface Configuration** page to configure specific interfaces with PIM.

To display the page, click **IPv4 Multicast > PIM > Interface Configuration** or **IPv6 Multicast > PIM > Interface Configuration** in the tree view.

Figure 12-36. PIM Interface Configuration



The **PIM Interface Configuration** page contains the following fields:

- **Interface** — Select the interface for which data is to be displayed or configured. You must have configured at least one router interface before configuring or displaying data for a PIM interface, otherwise an error message is displayed.
- **Admin Mode** — Select Enable or Disable from the drop-down menu to set the administrative status of PIM for the selected interface. The default is Disable.
- **Hello Interval** — Enter the number of seconds between PIM hello messages transmitted from the selected interface. The default value is 30. Valid values are 0 to 65535 seconds.
- **Join Prune Interval** — Enter the frequency at which PIM Join/Prune messages are transmitted on this PIM interface. The valid values are from (0 to 65535). The default value is 60.
- **BSR Border —** Indicates whether this interface is enabled or disables to act as a border for all PIM bootstrap messages. Bootstrap messages do not cross the BSR border.
- **DR Priority —** The Designated Router priority value. The router with the highest priority value is elected as the Designated Router. A shared-media such as Ethernet may have multiple PIM-SM routers connected to it. A single one of these routers, the DR, acts on behalf of directly connected hosts with respect to the PIM protocol. This field is applicable for PIM-SM only. The valid values are 0 to 2147483647.

Downloaded from www.Manualslib.com manuals search engine

Configuring PIM-DM for an Interface

1. Open the **PIM-DM Interface Configuration** page.
2. Select the interface to configure from the **Interface** field.
3. Modify the remaining fields as needed.
4. Click **Apply Changes**.

   The interface configuration is saved, and the device is updated.

Configuring PIM-DM for an Interface using the CLI Command

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide:*

- PIM-DM Commands

PIM-DM Interface Summary

Use the **PIM-DM Interface Summary** page to display a PIM interface and its settings.

To display the page, click **IPv4 Multicast > PIM > Interface Summary** or **IPv6 Multicast > PIM > Interface Summary** in the tree view.

Figure 12-37. PIM Interface Summary

Downloaded from www.Manualslib.com manuals search engine

The **PIM Interface Summary** page contains the following fields:

- **Interface** — Select the interface for which data is to be displayed. There must be configured at least one router interface before displaying data for a PIM interface, otherwise an error message displays.

Interface Parameters fields are:

- **Admin Mode** — Displays the administrative status of PIM for the selected interface.
- **Protocol State** — The operational state of the PIM protocol on this interface.
- **IP Address** — The IP address of the selected interface.
- **Hello Interval** — The frequency (in seconds) at which PIM hello messages are transmitted on the selected interface.
- **Join/Prune Interval** — The frequency (in seconds) at which PIM Join/Prune messages are transmitted on this PIM interface.
- **DR Priority** — Indicates the DR priority on the PIM interface. This field is supported in PIM-SM only.
- **BSR Border** — Specifies the BSR border mode on the PIM interface. This field is not supported for PIM-DM.
- **Designated Router** — The designated router on the selected PIM interface. For point-to-point interfaces, this is 0.0.0.0.

Interface Neighbors fields are:

- **Neighbor Count** — The number of PIM neighbors on the selected interface.
- **Neighbor IP** — The IP address of the PIM neighbor for which this entry contains information.
- **Up Time** (hh:mm:ss) — The time since this PIM neighbor (last) became a neighbor of the local router.

Expiry Time (hh:mm:ss) — The minimum time remaining before this PIM neighbor is aged out.

Displaying PIM-DM Interface Summary using the CLI Command

For information about the CLI command that performs this function, see the following chapter in the *CLI Reference Guide:*

- PIM-DM Commands

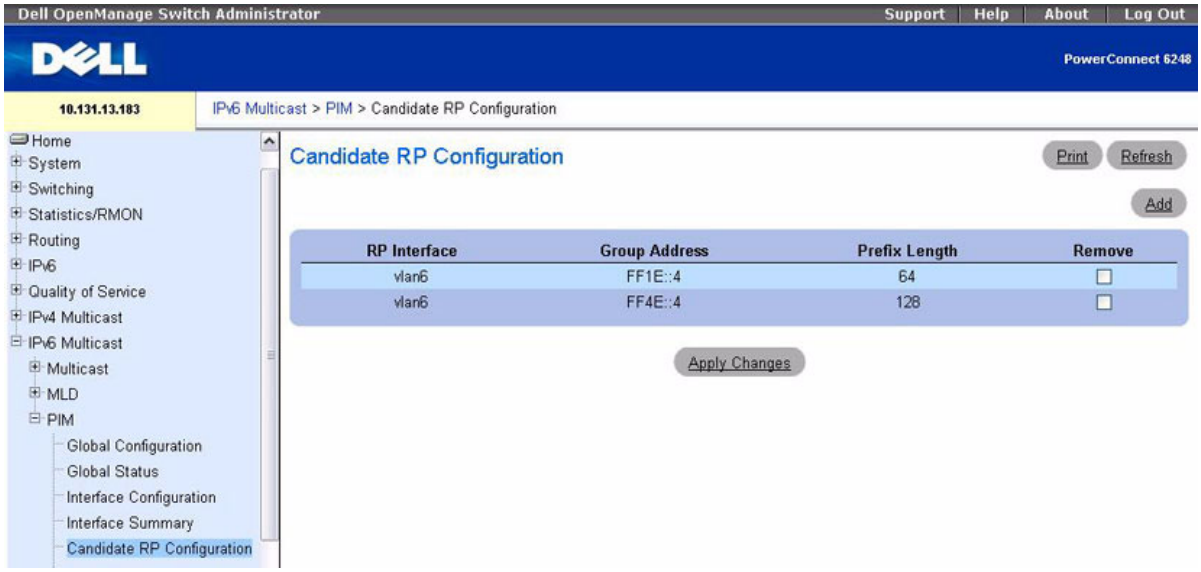
Downloaded from www.Manualslib.com manuals search engine

Candidate RP Configuration

The Candidate RP is configured on the Add Candidate RP page. Use the Candidate RP Configuration page to display and delete the configured rendezvous points (RPs) for each port using PIM.

To access the page, click **IPv4 Multicast > PIM > Candidate RP Configuration** or **IPv6 Multicast > PIM > Candidate RP Configuration**.

Figure 12-38. Candidate RP Configuration



The **Candidate RP Configuration** page contains the following fields:

- **RP Interface** — Displays the interface for which the Candidate RP data is to be displayed. Slot 0 is the base unit.
- **Group Address** — Displays the group address transmitted in Candidate-RP-Advertisements.
- **Group Mask** — (IPv4) Displays the group address mask transmitted in Candidate-RP-Advertisements to fully identify the scope of the group which the router supports if it is elected as a Rendezvous Point.
- **Prefix Length** — (IPv6) Displays the group address prefix length transmitted in Candidate-RP-Advertisements to fully identify the scope of the group which the router will support if it is elected as a Rendezvous Point.
- **Remove** — Select this option and click **Apply Changes** to remove the specified Candidate RP Address for the PIM router.

After entering all required data, click **Apply Changes** to configure an interface as a PIM candidate.

Downloaded from www.Manualslib.com manuals search engine

Configuring the Candidate RP using the CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide:*

- PIM Commands

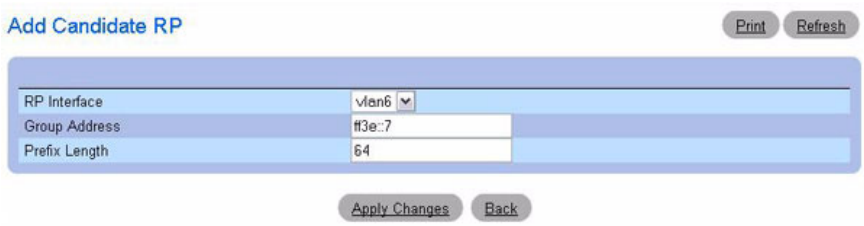
Adding a Candidate RP

Use the **Add Candidate RP** page to add PIM Candidate rendezvous points (RPs) for each IP multicast group.

1. Open the **Candidate RP Configuration** page.
2. Click **Add**.

   The **Add Candidate RP** page displays.

Figure 12-39. Add Candidate RP



3. Select the interface for which the Candidate RP is to be configured.
4. Enter the group address transmitted in Candidate-RP-Advertisements.
5. Enter the prefix length transmitted in Candidate-RP-Advertisements to fully identify the scope of the group which the router supports if elected as a Rendezvous Point.
6. Click **Apply Changes**.

   The new Candidate RP is added, and the device is updated.

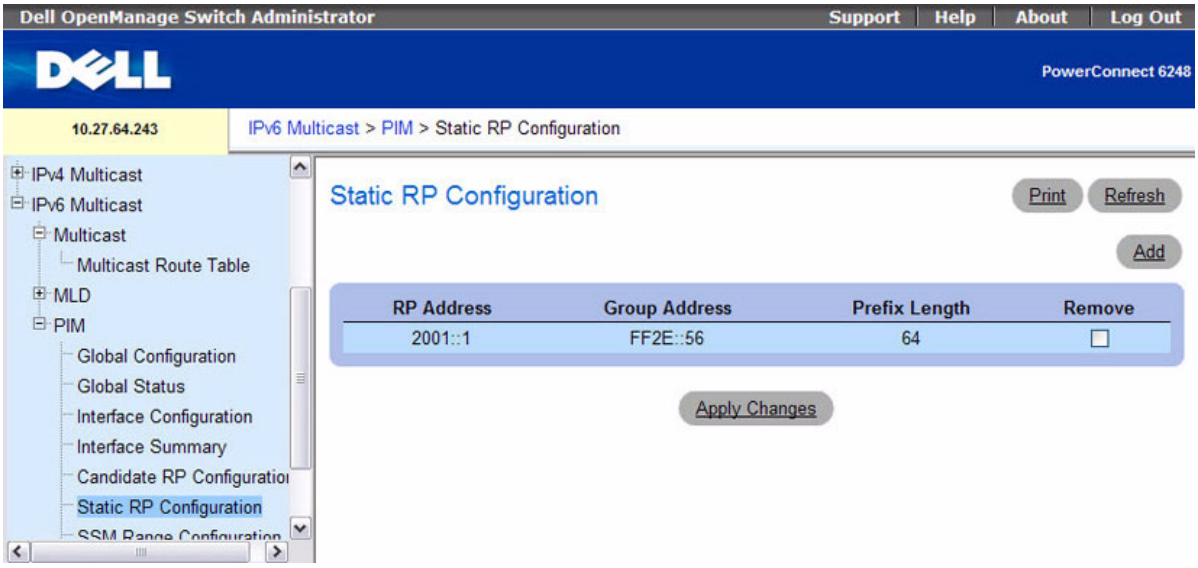
Downloaded from www.Manualslib.com manuals search engine

Static RP Configuration

Use the **PIM Static RP Configuration** page to display or remove the configured RP. The page also allows adding new static RPs by clicking the **Add** button.

To access the page, click **IPv4 Multicast > PIM > Static RP Configuration** or **IPv6 Multicast > PIM > Static RP Configuration**.

Figure 12-40. Static RP Configuration



The **Static RP Configuration** page contains the following fields:

- **RP Address** — Select the slot and port for which data is to be displayed. Slot 0 is the base unit.
- **Group Address** — Specify the group address transmitted in Candidate-RP-Advertisements in Prefix/Length format.
- **Group Mask** — (IPv4) The Group Mask of the RP to be created or deleted.
- **Prefix Length** — (IPv6) Specify the group address prefix length transmitted in Candidate-RP-Advertisements to fully identify the scope of the group which the router will support if elected as a Rendezvous Point.
- **Remove** — Select this box to remove the specified static RP IP Address for the PIM router.

After entering all required data, click **Apply Changes** to configure an interface as a PIM candidate.

Configuring the Candidate RP using the CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide:*

- PIM Commands

Downloaded from www.Manualslib.com manuals search engine

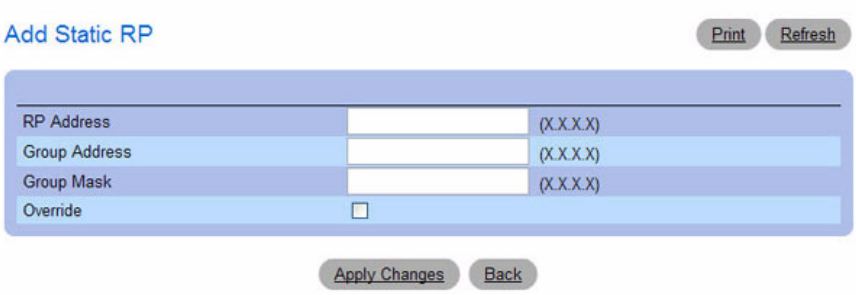
Adding a Static RP

Use the **Add Static RP** page to add the specified static rendezvous point (RP) for the PIM router.

1. Open the **Static RP Configuration** page.
2. Click **Add**.

   The **Add Static RP** page displays.

Figure 12-41. Add Static RP



3. Enter the IP address of the RP for the group range.
4. Enter the group address of the RP.
5. Enter the group mask of the RP.
6. Check the **Override** option to configure the static RP to override the dynamic (candidate) RPs learned for same group ranges.
7. Click **Apply Changes**.

   The new Static RP is added, and the device is updated.

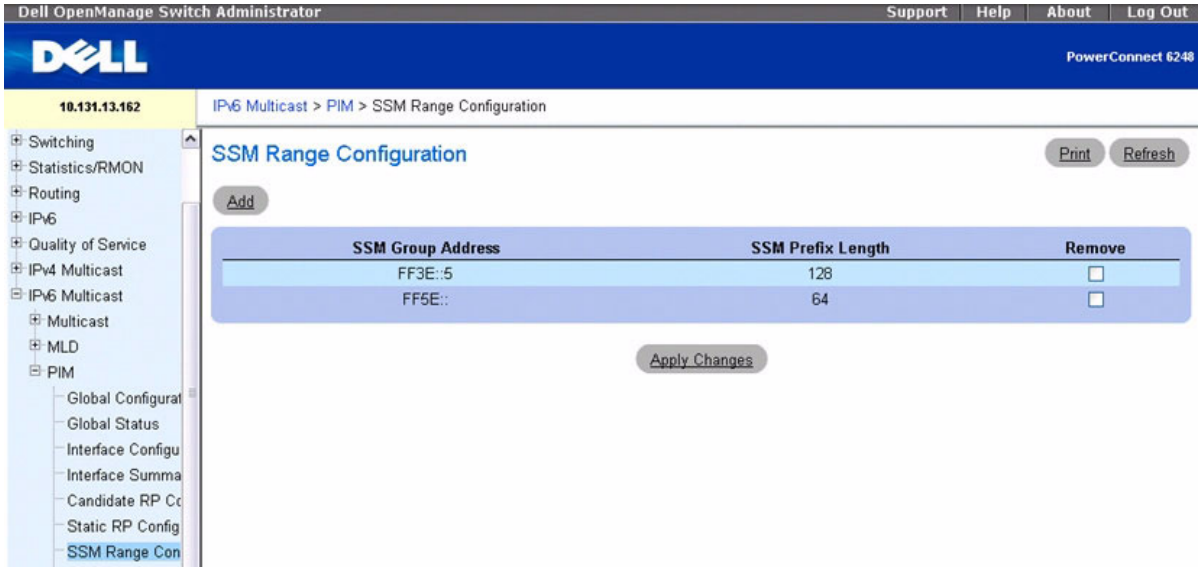
Downloaded from www.Manualslib.com manuals search engine

SSM Range Configuration

Use this page to display or remove the the Source Specific Multicast (SSM) group IP address and group mask for the PIM router.

To display the page, click **IPv4 Multicast > PIM > SSM Range Configuration** or **IPv6 Multicast > PIM > SSM Candidate Configuration**.

Figure 12-42. SSM Range Configuration



The **SSM Range Configuration** page contains the following fields:

- **SSM Group Address** — Displays the Source-Specific Multicast (SSM) group IP address.
- **SSM Group Mask** — (IPv4) Displays the SSM group ip-address mask.
- **SSM Prefix Length** — (IPv6) Displays the source-specific multicast group Prefix Length.
- **Remove** — Select this option and click **Apply Changes** to remove the specified SSM Group IP Addresses for the PIM router.

To configure the SSM Range, click the **Add** button to display the **SSM Range Configuration** page. Enter values for the **SSM Group Address** and **SSM Group Mask**, click **Apply Changes**, then the **Back** button.

Configuring the BSR Candidate using the CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide:*

- PIM Commands

Downloaded from www.Manualslib.com manuals search engine

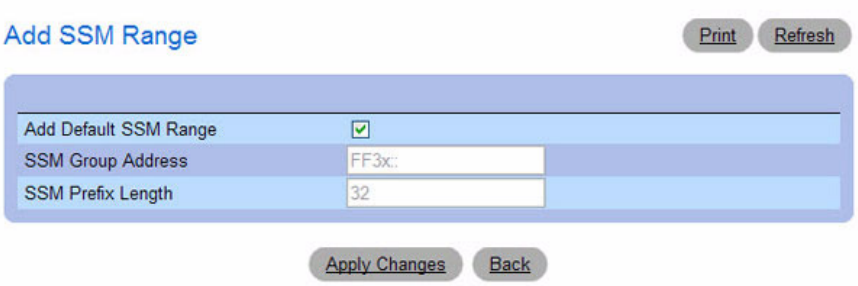
Adding an SSM Range

Use the **Add SSM Range** page to add the Source-Specific Multicast (SSM) Group IP Address and Group Mask (IPv4) or Prefix Length (IPv6) for the PIM router.

1. Open the **SSM Range Configuration** page.
2. Click **Add**.

   The **Add SSM Range** page displays.

Figure 12-43. Add SSM Range



3. Click the Add Default SSM Range check box to add the default SSM Range. The default SSM Range is ff3x::/32.
4. Enter the SSM Group IP Address.
5. Enter the SSM Group Mask (IPv4) or SSM Prefix Length (IPv6).
6. Click **Apply Changes**.

   The new SSM Range is added, and the device is updated.

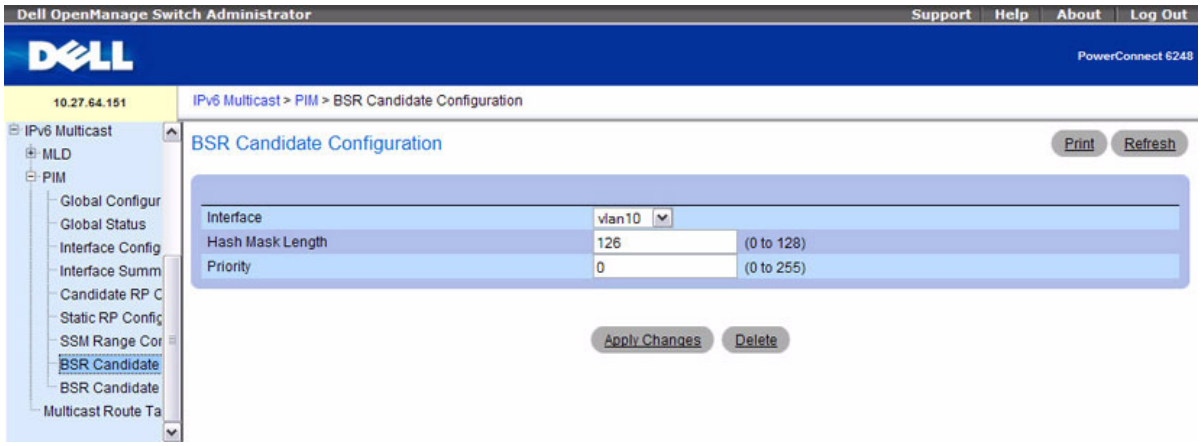
Downloaded from www.Manualslib.com manuals search engine

BSR Candidate Configuration

Use this page to configure information to be used if the interface is selected as a bootstrap router.

To display the page, click **IPv4 Multicast > PIM > BSR Candidate Configuration** or **IPv6 Multicast > PIM > BSR Candidate Configuration**.

Figure 12-44. BSR Candidate Configuration



The **BSR Candidate Configuration** page contains the following fields:

- **Interface** — Select the interface for which data is to be displayed.
- **Hash Mask Length** — The CBSR hash mask length to be advertised in bootstrap messages if this interface is elected as the bootstrap router. This hash mask length will be used in the hash algorithm for selecting the RP for a particular group. The valid values are from 0 to 128.The default value is 126.
- **Priority** — The priority value for the local interface as a candidate bootstrap router. The valid values are from 0 to 255.The default value is 0.

Configuring the BSR Candidate using the CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide:*

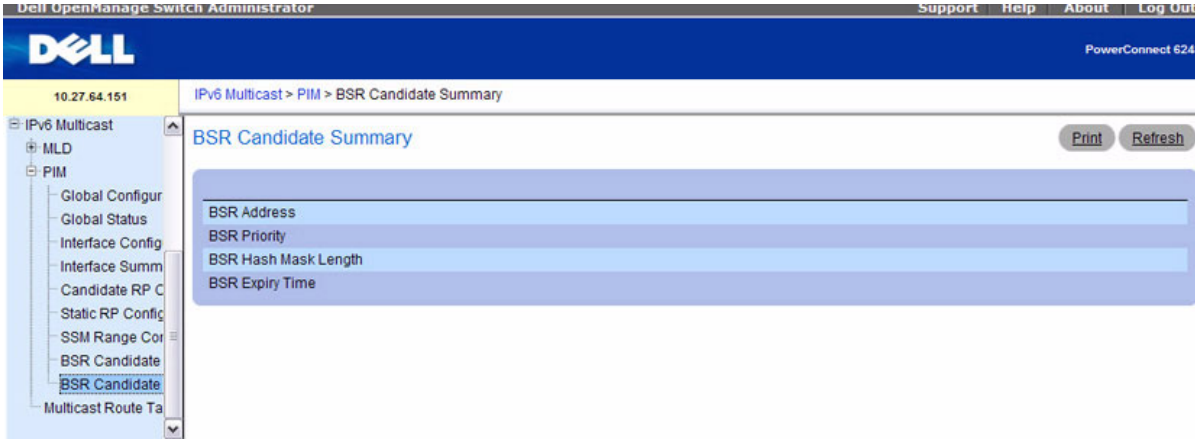
- PIM Commands

Downloaded from www.Manualslib.com manuals search engine

BSR Candidate Summary

Use this page to display information about the configured BSR candidates. To display this page, click **IPv4 Multicast > PIM > BSR Candidate Summary** or **IPv6 Multicast > PIM > BSR Candidate Summary**.

Figure 12-45. BSR Candidate Summary



The **BSR Candidate Summary** page contains the following fields:

- **BSR Address** — Displays the IP address of the elected bootstrap router (BSR).
- **BSR Priority** — Displays the priority value of the elected BSR.
- **BSR Hash Mask Length** — Displays the mask length of the elected BSR.
- **BSR Expiry Time** — Time (in hours, minutes, and seconds) in which the learned elected BootStrap Router (BSR) expires.

Viewing the BSR Candidate Summary using the CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide:*

- PIM Commands

Protocol Independent Multicast-Sparse Mode

Protocol Independent Multicast-Sparse Mode (PIM-SM) is used to efficiently route multicast traffic to multicast groups that may span wide area networks and where bandwidth is a constraint. PIM-SM uses shared trees by default and implements source-based trees for efficiency. This data threshold rate is used to toggle between trees. PIM-SM assumes that no hosts want the multicast traffic unless they specifically ask for it. It creates a shared distribution tree centered on a defined rendezvous point (RP) from which source traffic is relayed to the receivers. Senders first send the multicast data to the RP, which in turn

Downloaded from www.Manualslib.com manuals search engine

sends the data down the shared tree to the receivers. Shared trees centered on a RP do not necessarily provide the shortest/optimal path. In such cases, PIM-SM provides a means to switch to more efficient source-specific trees.

The **PIM-SM** menu page contains links to web pages that define and display PIM-SM parameters and data. To display this page, click **IP Multicast > PIM-SM** in the tree view.

Following are the web pages accessible from this menu page:

- PIM-SM Global Configuration
- PIM-SM Global Status
- PIM-SM Interface Configuration
- PIM-SM Interface Summary
- Component Summary
- RP Set Summary
- Candidate RP Summary
- Static RP Configuration

PIM-SM Global Configuration

Use the **PIM-SM Global Configuration** page to configure global PIM-SM settings for this system.

To display the page, click **Multicast > PIM-SM > Global Configuration** in the tree view.

Downloaded from www.Manualslib.com manuals search engine

Figure 12-46. PIM-SM Global Configuration

The **PIM-SM Global Configuration** page contains the following fields:

- **Admin Mode** — Select Enable or Disable from the drop-down menu to set the administrative status of PIM-SM on the system. You must enable IGMP before enabling PIM-SM. The default is Disable.
- **Join/Prune Interval (secs)** — Enter the interval between the transmission of PIM-SM Join/Prune messages. The valid values are from 10 to 3600 secs. The default value is 60.
- **Data Threshold Rate (Kbps)** — Enter the minimum source data rate in K bits/second above which the last-hop router switches to a source-specific shortest path tree. The valid values are from 0 to 2000 K bits/sec. The default value is 50.
- **Register Threshold Rate (Kbps)** — Enter the minimum source data rate in K bits/second above which the Rendezvous Point router switches to a source-specific shortest path tree. The valid values are from 0 to 2000 K bits/sec. The default value is 50.

Configuring PIM-SM

1. Open the **PIM-SM Global Configuration** page.
2. Set **Admin Mode** to Enable or Disable, to turn PIM-SM on or off.
3. Modify the remaining fields as needed.
4. Click **Apply Changes**.

Downloaded from www.Manualslib.com manuals search engine

The interface configuration is saved, and the device is updated.

Configuring PIM-SM using the CLI Command

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide:*

- PIM-SM Commands

Downloaded from www.Manualslib.com manuals search engine

PIM-SM Global Status

Use the **PIM-SM Global Status** page to display the global settings selected on the **PIM-SM Global Configuration** page.

To display the page, click **Multicast > PIM-SM > Global Status** in the tree view.

Figure 12-47. PIM-SM Global Status

The **PIM-SM Global Status** page displays the following fields:

- **Admin Mode** — The administrative status of PIM-SM in the router: either Enable or Disable.
- **Join/Prune Interval (secs)** — The interval between the transmission of PIM-SM Join/Prune messages.
- **Data Threshold Rate (Kbps)** — The minimum source data rate in K bits/second above which the last-hop router switches to a source-specific shortest path tree.
- **Register Threshold Rate (Kbps)** — The minimum source data rate in K bits/second above which the Rendezvous Point router switches to a source-specific shortest path tree.

Displaying PIM-SM Global Status using the CLI Command

For information about the CLI command that performs this function, see the following chapter in the *CLI Reference Guide:*

- PIM-SM Commands

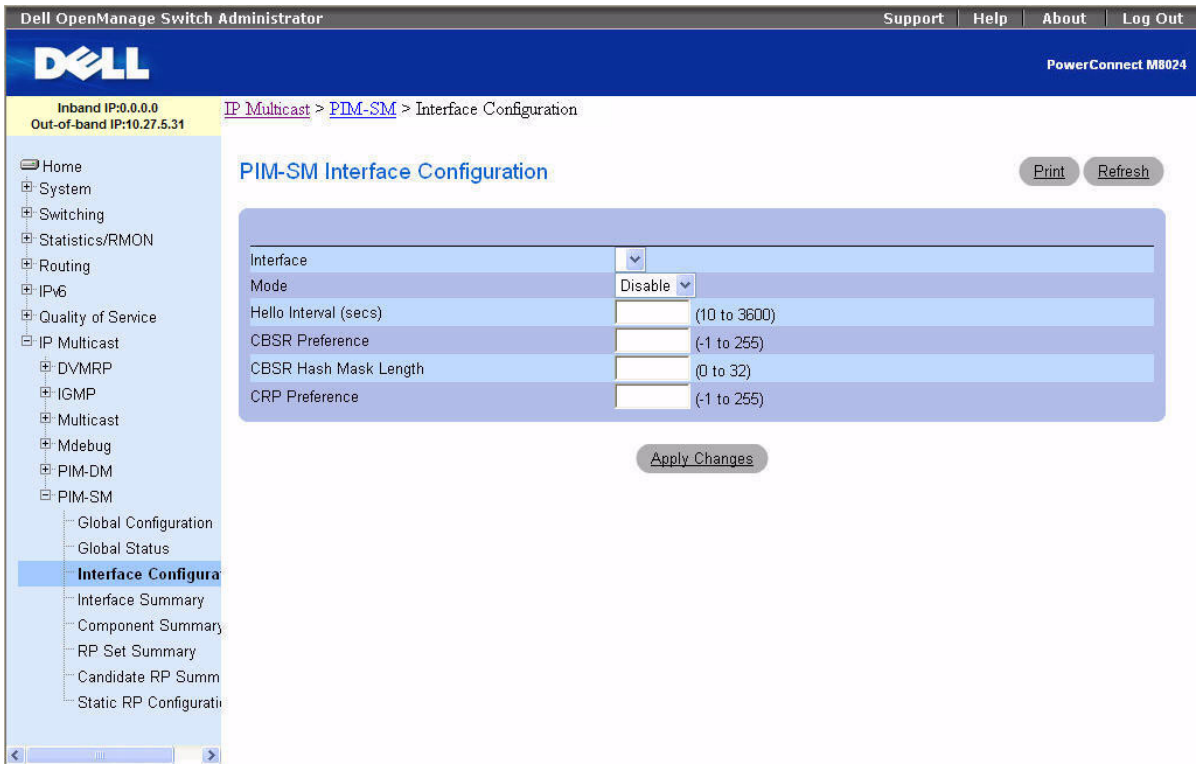
Downloaded from www.Manualslib.com manuals search engine

PIM-SM Interface Configuration

Use the **PIM-SM Interface Configuration** page to configure PIM-SM for an interface. PIM-SM must be enabled on the **PIM-SM Global Configuration** page for this interface configuration page to display.

To display the page, click **Multicast > PIM-SM > Interface Configuration** in the tree view.

Figure 12-48. PIM-SM Interface Configuration



The **PIM-SM Interface Configuration** page contains the following fields:

- **Interface** — Select the interface for which data is to be displayed or configured. At least one routing interface must exist in order to display or configure data.
- **Mode** — Select Enable or Disable from the drop-down menu to set the administrative status of PIM-SM on this interface. The default is Disable.
- **Hello Interval (secs)** — Enter the time in seconds between the transmission of which PIM Hello messages on this interface. The valid values are from 10 to 3600 secs. The default value is 30.
- **CBSR Preference** — Enter the preference value for the local interface as a candidate bootstrap router. The value of -1 is used to indicate that the local interface is not a candidate BSR interface. The valid values are from -1 to 255. The default value is 0.

Downloaded from www.Manualslib.com manuals search engine

- **CBSR Hash Mask Length** — Enter the CBSR hash mask length to be advertised in bootstrap messages if this interface is elected as the bootstrap router. This hash mask length is used in the hash algorithm for selecting the RP for a particular group. The valid values are from 0 to 32. The default value is 30.
- **CRP Preference** — Enter the preference value for the local interface as a candidate bootstrap router. The value of -1 is used to indicate that the local interface is not a candidate BSR interface. The valid values are from -1 to 255. The default value is 0.

Configuring PIM-SM for an Interface

1. Open the **PIM-SM Interface Configuration** page.
2. Select the interface to configure from the **Interface** field.
3. Select **Enable** from the **Mode** field.
4. Modify the remaining fields as needed.
5. Click **Apply Changes**.

   The interface configuration is saved, and the device is updated.

Configuring PIM-SM for an Interface using the CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide:*

- PIM-SM Commands

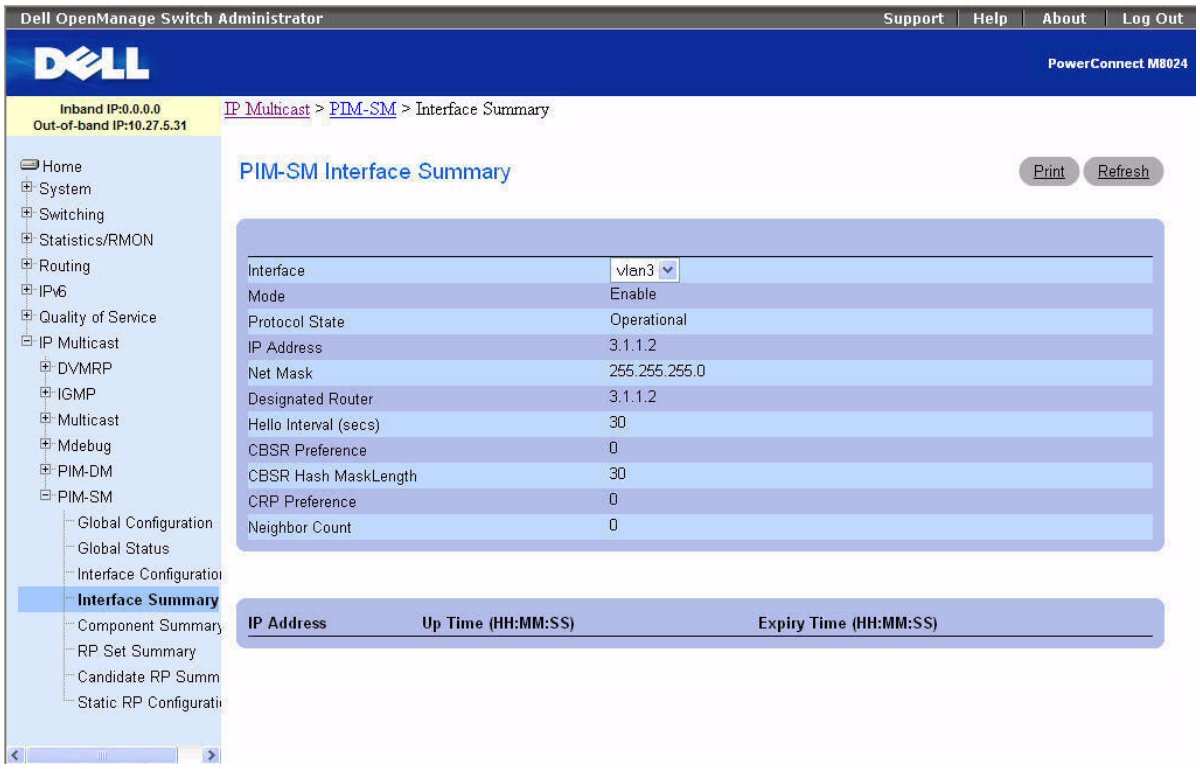
Downloaded from www.Manualslib.com manuals search engine

PIM-SM Interface Summary

Use the **PIM-SM Interface Summary** page to display a PIM-SM interface and its settings. At least one interface on this router must be set up as PIM-SM for this page to display.

To display the page, click **Multicast > PIM-SM > Interface Summary** in the tree view.

Figure 12-49. PIM-SM Interface Summary



The **PIM-SM Interface Summary** page displays the following fields:

- **Interface** — Select the interface for which data is to be displayed.
- **Mode** — The administrative status of PIM-SM in the router: either Enable or Disable.
- **Protocol State** — The operational state of the PIM-SM protocol on the selected interface, either Operational or Non-operational.
- **IP Address** — The IP address of the selected PIM interface.
- **Net Mask** — The network mask for the IP address of the selected PIM interface.
- **Designated Router** — The Designated Router on the selected PIM interface. For point-to- point interfaces, this object has the value 0.0.0.0.
- **Hello Interval (secs)** — The frequency at which PIM Hello messages are transmitted on the selected interface.

Downloaded from www.Manualslib.com manuals search engine

- **CBSR Preference** — The preference value for the local interface as a candidate bootstrap router. The value of -1 is used to indicate that the local interface is not a candidate BSR interface.
- **CBSR Hash Mask Length** — The CBSR hash mask length to be advertised in bootstrap messages if this interface is elected as the bootstrap router. This hash mask length is used in the hash algorithm for selecting the RP for a particular group.
- **CRP Preference** — The preference value for the local interface as a candidate bootstrap router. The value of -1 is used to indicate that the local interface is not a candidate BSR interface.
- **Neighbor Count** — The number of PIM neighbors on the selected interface.
- **IP Address** — The IP address of the PIM neighbor for this entry.
- **Up Time (hh:mm:ss)** — The time since this PIM neighbor (last) became a neighbor of the local router.
- **Expiry Time (hh:mm:ss)** — The minimum time remaining before this PIM neighbor is aged out.

Displaying PIM-SM Interface Summary

1. Open the **PIM-SM Interface Summary** page.
2. Select the interface to display from the **Interface** drop-down menu.

   PIM-SM configuration data for this interface displays.

Displaying PIM-SM Interface Summary using the CLI Command

For information about the CLI command that performs this function, see the following chapter in the *CLI Reference Guide:*

- PIM-SM Commands

Downloaded from www.Manualslib.com manuals search engine

Component Summary

Use the **Component Summary** page to display PIM-SM component data.

To display the page, click **Multicast > PIM-SM > Component Summary** in the tree view.

Figure 12-50. Component Summary

The **Component Summary** page displays the following fields:

- **Component Index** — Unique number identifying the component index.
- **Component BSR Address** — The IP address of the bootstrap router (BSR) for the local PIM region.
- **Component BSR Expiry Time (hh:mm:ss)** — The minimum time remaining before the bootstrap router in the local domain is declared.
- **Component CRP Hold Time (hh:mm:ss)** — The hold time of the component when it is a candidate Rendezvous Point in the local domain.

Displaying PIM-SM Component Summary using the CLI Command

For information about the CLI command that performs this function, see the following chapter in the *CLI Reference Guide:*

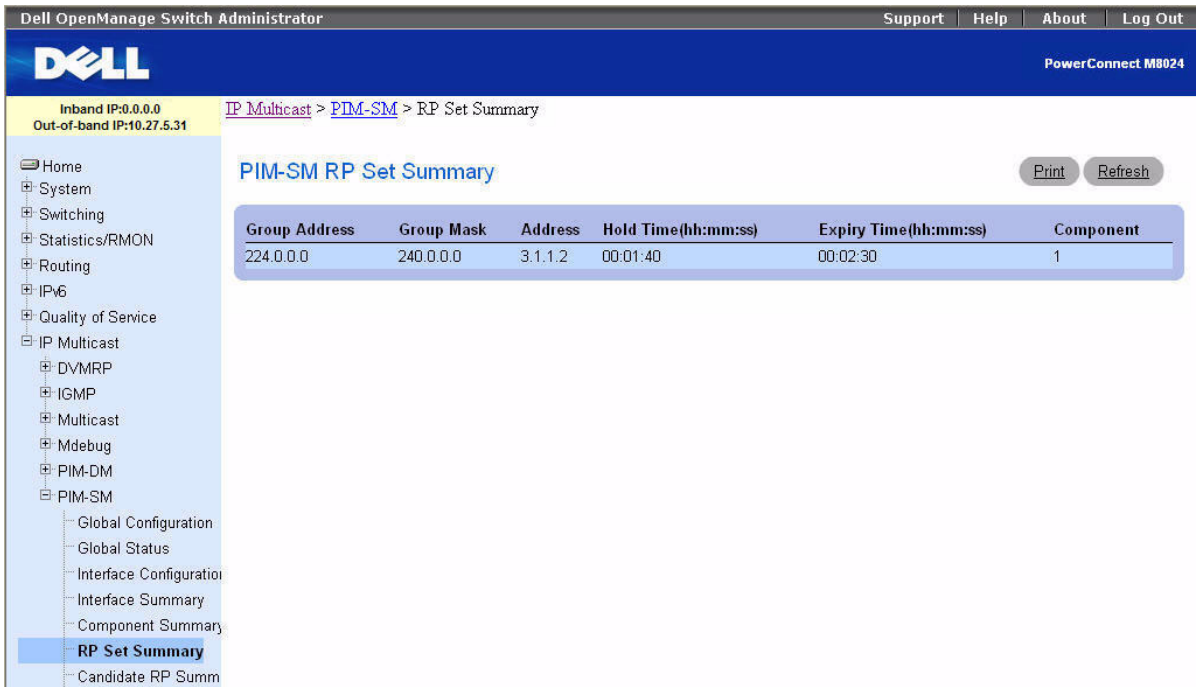
- PIM-SM Commands

Downloaded from www.Manualslib.com manuals search engine

RP Set Summary

Use the **PIM-SM RP Set Summary** page to display the static RP information for the PIM-SM router. To display the page, click **Multicast > PIM-SM > RP Set Summary** in the tree view.

Figure 12-51. PIM-SM RP Set Summary



The **PIM-SM RP Set Summary** page displays the following fields in a table:

- **Group Address** — Displays IP multicast group address.
- **Group Mask** — Displays Multicast group address mask.
- **Address** — Displays IP address of the Candidate-RP.
- **Hold Time (hh:mm:ss)** — The holdtime of a Candidate-RP. If the local router is not the BSR, this value is 0.
- **Expiry Time (hh:mm:ss)** — The minimum time remaining before the Candidate-RP is declared down.
- **Component** — A number which uniquely identifies the component. Each protocol instance connected to a separate domain should have a different index value.

Displaying RP Set Summary using the CLI Commands

For information about the CLI commands that perform this function, see the following chapter in the *CLI Reference Guide:*

- PIM-SM Commands

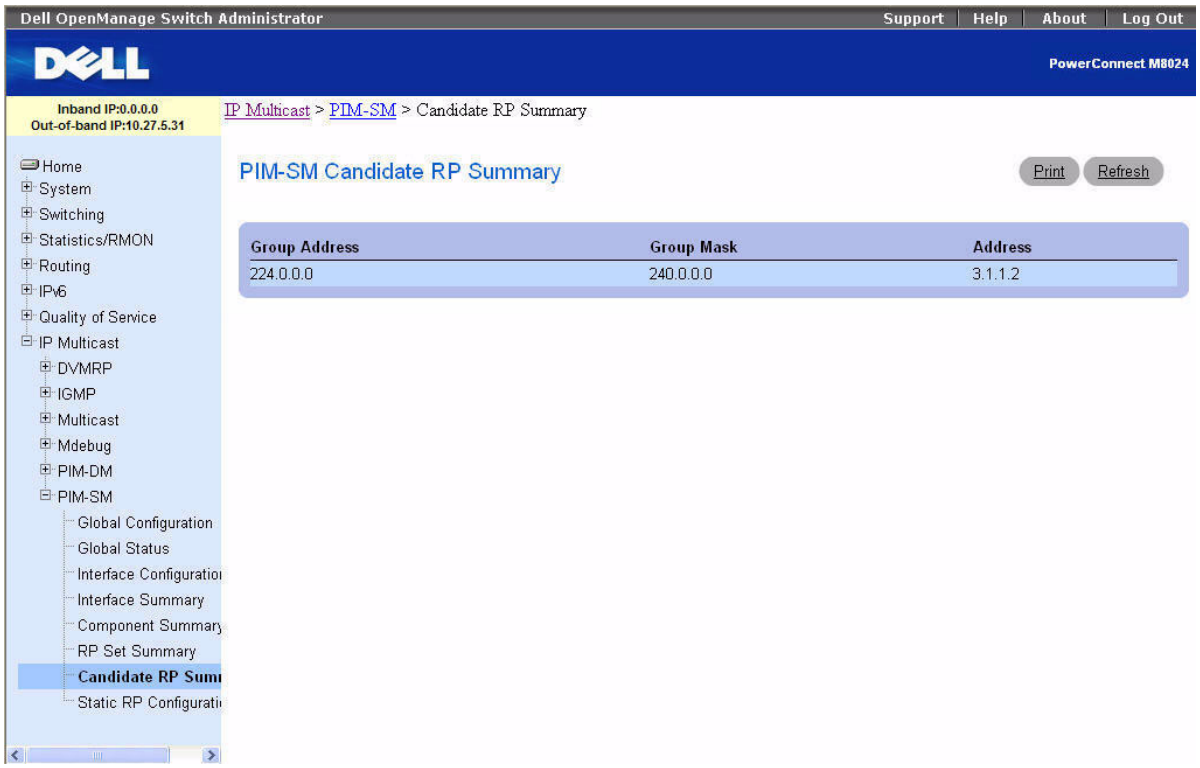
Downloaded from www.Manualslib.com manuals search engine

Candidate RP Summary

Use the **PIM-SM Candidate RP Summary** page to display PIM information for candidate Rendezvous Points (RPs) for each IP multicast group.

To display the page, click **Multicast > PIM-SM > Candidate RP Summary** in the tree view.

Figure 12-52. PIM-SM Candidate RP Summary



The **PIM-SM Candidate RP Summary** page displays the following fields in a table:

- **Group Address** — The group address transmitted in Candidate-RP-Advertisements.
- **Group Mask** — The group address mask transmitted in Candidate-RP-Advertisements to fully identify the scope of the group which the router supports if elected as a Rendezvous Point.
- **Address** — Displays the unicast address of the interface which is advertised as a Candidate RP.

Displaying PIM-SM Candidate RP Summary using the CLI Command

For information about the CLI command that performs this function, see the following chapter in the *CLI Reference Guide:*

- PIM-SM Commands

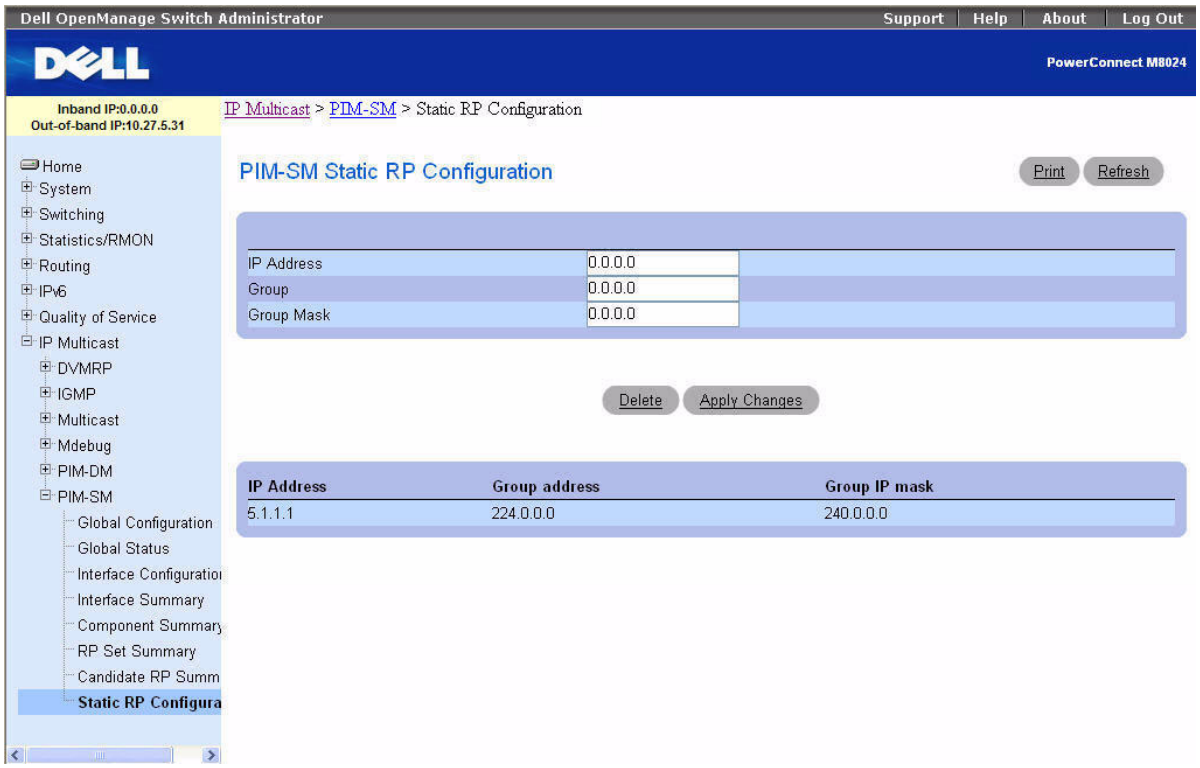
Downloaded from www.Manualslib.com manuals search engine

Static RP Configuration

Use the **Static RP Configuration** page to create the specified static RP IP Address for the PIM-SM router.

To display the page, click **Multicast** > **PIM-SM** > **Static RP Configuration** in the tree view.

Figure 12-53. Static RP Configuration



The **Static RP Configuration** page contains the following fields:

- **IP Address** — IP Address of the RP to be created.
- **Group** — Group Address of the RP to be created.
- **Group Mask** — Group IP Mask of the RP to be created.

Existing configurations display in a table at the bottom of the page.

Configuring Static RP

1. Open the **Static RP Configuration** page.
2. Enter the **IP Address**, the IP address for the **Group**, and the **Group Mask** for the static RP configuration.
3. Click **Apply Changes**.

   The specified static RP IP Address for the PIM-SM router is created, and the device is updated.

Downloaded from www.Manualslib.com manuals search engine

Configuring Static RP using the CLI Command

For information about the CLI command that performs this function, see the following chapter in the *CLI Reference Guide:*

- PIM-SM Commands

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

13

Getting Help

This section contains information about getting help for questions about the Dell™ PowerConnect™ M6220/M6348/M8024. The topics covered in this section include:

- Obtaining Assistance
- Dell Enterprise Training and Certification
- Problems With Your Order
- Product Information
- Returning Items for Warranty Repair or Credit
- Before You Call
- Contacting Dell

Downloaded from www.Manualslib.com manuals search engine

Obtaining Assistance

If you experience a problem with your computer, you can complete the following steps to diagnose and troubleshoot the problem:

1. Fill out the "Diagnostics Checklist" on page 733.
2. Use Dell's extensive suite of online services available at Dell Support (**support.dell.com**) for help with installation and troubleshooting procedures. See "Online Services" on page 730 for a more extensive list of Dell Support online.
3. If the preceding steps have not resolved the problem, see "Contacting Dell" on page 734.

Note: Call Dell Support from a telephone near or at the computer so that the support staff can assist you with any necessary procedures.

Note: Dell's Express Service Code system may not be available in all countries.

When prompted by Dell's automated telephone system, enter your Express Service Code to route the call directly to the proper support personnel. If you do not have an Express Service Code, open the **Dell Accessories** folder, double-click the **Express Service Code** icon, and follow the directions.

For instructions on using the Dell Support, see "Support Service" on page 731.

Note: Some of the following services are not always available in all locations outside the continental U.S. Call your local Dell representative for information on availability.

Online Services

You can learn about Dell products and services on the following websites:

www.dell.com

www.dell.com/ap (Asian/Pacific countries only)

www.dell.com/jp (Japan only)

www.euro.dell.com (Europe only)

www.dell.com/la (Latin American and Caribbean countries)

www.dell.ca (Canada only)

You can access Dell Support through the following websites and e-mail addresses:

- Dell Support websites

  support.dell.com

  support.jp.dell.com (Japan only)

  support.euro.dell.com (Europe only)

Downloaded from www.Manualslib.com manuals search engine

- Dell Support e-mail addresses

  mobile_support@us.dell.com

  support@us.dell.com

  la-techsupport@dell.com (Latin America and Caribbean countries only)

  apsupport@dell.com (Asian/Pacific countries only)
- Dell Marketing and Sales e-mail addresses

  apmarketing@dell.com (Asian/Pacific countries only)

  sales_canada@dell.com (Canada only)
- Anonymous file transfer protocol (FTP)

  ftp.dell.com

  Log in as user: `anonymous`, and use your e-mail address as your password.

Automated Order-Status Service

To check on the status of any Dell products that you have ordered, you can go to **support.dell.com**, or you can call the automated order-status service. A recording prompts you for the information needed to locate and report on your order. For the telephone number to call for your region, see "Contacting Dell" on page 734.

Support Service

Dell's support service is available 24 hours a day, 7 days a week, to answer your questions about Dell hardware. Our support staff use computer-based diagnostics to provide fast, accurate answers.

To contact Dell's support service, see "Before You Call" on page 732 and then see the contact information for your region.

Dell Enterprise Training and Certification

Dell Enterprise Training and Certification is available; see **www.dell.com/training** for more information. This service may not be offered in all locations.

Problems With Your Order

If you have a problem with your order, such as missing parts, wrong parts, or incorrect billing, contact Dell for customer assistance. Have your invoice or packing slip handy when you call. For the telephone number to call for your region, see "Contacting Dell" on page 734.

Downloaded from www.Manualslib.com manuals search engine

Product Information

If you need information about additional products available from Dell, or if you would like to place an order, visit the Dell website at **www.dell.com**. For the telephone number to call for your region or to speak to a sales specialist, see "Contacting Dell" on page 734.

Returning Items for Warranty Repair or Credit

Prepare all items being returned, whether for repair or credit, as follows:

1. Call Dell to obtain a Return Material Authorization Number, and write it clearly and prominently on the outside of the box.

   For the telephone number to call for your region, see "Contacting Dell" on page 734.

2. Include a copy of the invoice and a letter describing the reason for the return.
3. Include a copy of the Diagnostics Checklist (see "Diagnostics Checklist" on page 733), indicating the tests that you have run and any error messages reported by the Dell Diagnostics.
4. Include any accessories that belong with the item(s) being returned (such as power cables, media such as CDs and diskettes, and guides) if the return is for credit.
5. Pack the equipment to be returned in the original (or equivalent) packing materials.

You are responsible for paying shipping expenses. You are also responsible for insuring any product returned, and you assume the risk of loss during shipment to Dell. Collect On Delivery (C.O.D.) packages are not accepted.

Returns that are missing any of the preceding requirements will be refused at Dell's receiving dock and returned to you.

Before You Call

Note: Have your Express Service Code ready when you call. The code helps Dell's automated-support telephone system direct your call more efficiently.

Remember to fill out the Diagnostics Checklist (see "Diagnostics Checklist" on page 733). If possible, turn on your computer before you call Dell for assistance and call from a telephone at or near the computer. You may be asked to type some commands at the keyboard, relay detailed information during operations, or try other troubleshooting steps possible only at the computer itself. Ensure that the computer documentation is available.

Before working inside your switch, follow the safety instructions in your *Product Information Guide*.

Downloaded from www.Manualslib.com manuals search engine

Diagnostics Checklist

Name:

Date:

Address:

Phone number:

Service Tag (bar code on the back or bottom of the computer):

Express Service Code:

Return Material Authorization Number (if provided by Dell support technician):

Operating system and version:

Devices:

Expansion cards:

Are you connected to a network? Yes No

Network, version, and network adapter:

Programs and versions:

See your operating system documentation to determine the contents of the system's start-up files. If the computer is connected to a printer, print each file. Otherwise, record the contents of each file before calling Dell.

Error message, beep code, or diagnostic code:

Description of problem and troubleshooting procedures you performed:

Downloaded from www.Manualslib.com manuals search engine

Contacting Dell

For customers in the United States, call 800-WWW.DELL (800.999.3355).

Note: If you do not have an active Internet connection, you can find contact information on your purchase invoice, packing slip, bill, or Dell product catalog.

Dell provides several online and telephone-based support and service options. Availability varies by country and product, and some services may not be available in your area. To contact Dell for sales, technical support, or customer service issues:

1. Visit **support.dell.com**.
2. Verify your country or region in the **Choose A Country/Region** drop-down menu at the bottom of the page.
3. Click **Contact Us** on the left side of the page.
4. Select the appropriate service or support link based on your need.
5. Choose the method of contacting Dell that is convenient for you.

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine